TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 7817-3 : 2007

ISO/IEC 11770-3 : 1999

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - KỸ THUẬT MẬT MÃ QUẢN LÝ KHOÁ - PHẦN 3: CÁC CƠ CHẾ SỬ DỤNG KỸ THUẬT KHÔNG ĐỐI XỨNG

Information technology – Cryptographic technique - Key management

Part 3: Mechanisms using asymmetric techniques

HÀ NỘI – 2007

Mục lục

Trang

Lời nói đầu

TCVN 7817-3 : 2007 hoàn toàn tương đương với **ISO/IEC 11770-3 : 1999**

TCVN 7817-3 : 2007 do Tiểu ban Kỹ thuật Tiêu chuẩn TCVN/JTC 1/SC 27 "Các kỹ thuật mật mã" biên soạn, Ban Cơ yếu Chính phủ đề nghị, Bộ khoa học và công nghệ công bố

Xuất bản lần 1

Công nghệ thông tin – Kỹ thuật mật mã – Quản lý khóa Phần3 : Các cơ chế sử dụng kỹ thuật phi đối xứng

Information technology – Cryptographic techniques – Key management
Part 3: Mechanisms using asymmetric techniques

1 Phạm vi áp dụng

Tiêu chuẩn này xác định các cơ chế quản lý khóa dựa trên kỹ thuật mật mã phi đối xứng. Đặc biệt, nó sử dụng các kỹ thuật phi đối xứng để đạt được các mục tiêu sau:

1. Thiết lập khóa bí mật dùng chung sử dụng cho kỹ thuật mật mã đối xứng giữa hai thực thể *A* và *B* bằng việc thỏa thuận khóa. Trong một cơ chế thỏa thuận khóa bí mật thì khóa bí mật là kết quả của việc trao đổi dữ liệu giữa hai thực thể *A* và *B*. Không thể nào trong hai thực thể có thể định trước giá trị của khóa bí mật dùng chung này.

2. Thiết lập khóa bí mật dùng chung cho kỹ thuật mật mã đối xứng giữa hai thực thể *A* và *B* bằng việc vận chuyển khóa. Trong một cơ chế vận chuyển khóa bí mật thì khóa bí mật được chọn bởi một thực thể *A* được truyền đến thực thể *B*, quá trình vận chuyển khóa được bảo vệ một cách thích hợp bằng các kỹ thuật phi đối xứng.

3. Làm cho khóa công khai của một thực thể sẵn có đối với một thực thể khác bằng việc vận chuyển khóa. Trong cơ chế vận chuyển khóa công khai, một khóa công khai của thực thể *A* được truyền đến một thực thể khác theo một phương thức có xác thực nhưng không bắt buộc phải giữ bí mật.

Một số cơ chế trong tiêu chuẩn này dựa trên các cơ chế xác thực tương ứng ở ISO/IEC 9798-3.

Tiêu chuẩn này không đề cập đến các khía cạnh về quản lý khóa sau:

- Quản lý vòng đời của khóa,
- Các cơ chế sinh ra hoặc kiểm tra cặp khóa phi đối xứng,
- Các cơ chế dự trữ, lưu trữ, xóa, hủy,... khóa.

Mặc dù tiêu chuẩn này không đề cập cụ thể đến việc phân phối khóa bí mật từ bên thứ ba tin cậy đến một thực thể (trong một cặp khóa phi đối xứng) yêu cầu khóa nhưng mô tả về các cơ chế vận chuyển khóa ở đây vẫn có thể được sử dụng để đạt được mục tiêu phân phối khóa bí mật.

Tiêu chuẩn này cũng không đề cập đến việc thực thi các phép biến đổi sử dụng trong các cơ chế thỏa thuận khóa.

CHÚ THÍCH: Để đạt được tính xác thực của các thông điệp quản lý khóa thì có thể tạo một dự trữ sẵn về tính xác thực bên trong giao thức thiết lập khóa hoặc sử dụng hệ thống chữ ký khóa công khai để ký các thông điệp trao đổi khóa.

2 Tài liệu viện dẫn

Các tài liệu viễn dẫn dưới đây rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng bản mới nhất, bao gồm cả các sửa đổi.

- ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture (Các hệ thống xử lý thông tin - Liên kết các Hệ thống mở - Mô hình tham chiếu cơ bản – Phần 2: Cấu trúc an toàn).

- ISO/IEC 9594-8:1995, Information technology – Open systems Interconnection - The directory: Authentication framework (Công nghệ thông tin – Liên kết các Hệ thống mở - Thư mục: Khung xác thực).

- ISO/IEC 9798-3:1998, Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques (Công nghệ thông tin - Kỹ thuật mật mã - Xác thực thực thể - Phần 3: Các cơ chế sử dụng kỹ thuật chữ ký số).

- ISO/IEC 10118-1:1994, Information technology- Security techniques - Hash-functions- Part 1: General (Công nghệ thông tin - Kỹ thuật mật mã - Hàm băm - Phần 1: Tổng quát).

- ISO/IEC10181-1:1996, Information technology – Open systems Interconnection - Security frameworks for open systems Overview (Công nghệ thông tin - Liên kết các Hệ thống mở - Tổng quát về khung an toàn cho các hệ thống mở).

- TCVN 11770-1 : 2007(ISO/IEC 11770-1:1999), Information technology - Security techniques - Key management - Part 1: Frameworks (Công nghệ thông tin - Kỹ thuật mật mã - Quản lý khoá - Phần 1:Khung tổng quát).

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các định nghĩa sau:

3.1

Kỹ thuật mật mã phi đối xứng (asymmetric cryptographic technique)

Kỹ thuật mật mã sử dụng hai phép biến đổi có liên quan đến nhau, phép biến đổi công khai (được xác định bởi một khóa công khai) và phép biến đổi bí mật (được xác định bởi một khóa bí mật). Cả hai phép biến đổi này có đặc tính là khi đã biết phép biến đổi công khai cũng không thể tính toán ra được phép biến đổi bí mật.

CHÚ THÍCH: Một hệ thống dựa trên kỹ thuật mật mã phi đối xứng có thể là một hệ mật, một hệ chữ ký, một hệ thống kết hợp giữa hệ mật và hệ chữ ký hoặc một hệ thống thỏa thuận khóa. Có bốn phép biến đổi cơ bản đối với kỹ thuật mật mã phi đối xứng: ký và kiểm tra chữ ký cho hệ chữ ký, mã hóa và giải mã cho hệ mật. Phép biến đổi ký và phép giải mã được giữ bí mật bởi thực thể sở hữu nó trong khi phép mã hóa và phép kiểm tra chữ ký lại được công bố. Tồn tại một số hệ mật phi đối xứng (như RSA) mà bốn hàm cơ bản có thể được thực hiện chỉ nhờ hai phép chuyển đổi: một phép biến đổi bí mật dùng cho cả ký và giải mã thông điệp, một phép biến đổi công khai dùng cho cả kiểm tra và mã hóa thông điệp. Tuy nhiên, vì điều này không tuân theo nguyên tắc tách bạch khóa theo chức năng, bởi vậy trong tiêu chuẩn này bốn phép biến đổi cơ sở và các khóa tương ứng đều được tách bạch.

3.2

Hệ mã hóa phi đối xứng (asymmetric encipherment system)

Một hệ thống dựa trên kỹ thuật mật mã phi đối xứng trong đó một phép biến đổi công khai được sử dụng để mã hóa và một phép biến đổi bí mật được sử dụng để giải mã.

3.3 Cặp khóa phi đối xứng (asymmetric key pair): Một cặp của các khóa liên quan trong đó một khóa riêng xác định một phép biến đổi bí mật và khóa công khai xác định một phép biến đổi công khai.

3.4

Tổ chức chứng thực (CA – certification authority)

Trung tâm được tin cậy tạo và gán các chứng chỉ khóa công khai. Theo tùy chọn, CA có thể đảm nhận việc tạo và gán khóa cho các thực thể.

3.5

Hàm kiểm tra mật mã (cryptographic check function)

Phép biến đổi mật mã nhận đầu vào là một khóa bí mật và một chuỗi tùy ý, cho đầu ra là một giá trị kiểm tra mật mã. Việc tính toán một giá trị kiểm tra đúng mà không biết khóa mã là không thể thực hiện được [ISO/IEC 9798-1:1997].

3.6

Giá trị kiểm tra mật mã (cryptographic check value)

Thông tin nhận được bắt nguồn bằng việc trình bầy một phép biến đổi mật mã trên một đơn vị dữ liệu [ISO/IEC 9798-4:1995].

3.7

Giải mã (dicipherment)

Phép nghịch đảo của phép mã hóa tương ứng [TCVN 7817-1 : 2007(ISO/IEC 11770-1:1996)].

3.8

Chữ ký số (digital signiture)

Dữ liệu được thêm vào, hoặc là phép biến đổi mật mã của một đơn vị dữ liệu mà cho phép người nhận đơn vị dữ liệu chứng minh được nguồn gốc và tính toàn vẹn của đơn vị dữ liệu và bảo vệ người gửi và người nhận của đơn vị dữ liệu chống lại sự giả mạo của bên thứ ba, và người gửi được bảo vệ chống lại sự giả mạo bên nhận.

3.9

Thẻ định danh phân biệt (distinguishing identifier)

Thông tin phân biệt một cách rõ ràng một thực thể [TCVN 7817-1 : 2007 (ISO/IEC 11770-1:1996)].

3.10

Mã hóa (encipherment)

Phép biến đổi khả nghịch (có ngược) của dữ liệu bằng một thuật toán mật mã để tạo ra bản mã, tức là để dấu nội dung thông tin của dữ liệu [TCVN 7817-1 : 2007 (ISO/IEC 11770-1:1996)].

3.11

Xác thực thực thể (entity authentication)

Sự chứng nhận rằng một thực thể là thực thể được tuyên bố [ISO/IEC 9798-1:1997].

3.12

Xác thực thực thể của A đối với B (entity authentication of A to B)

Sự đảm bảo về định danh của thực thể A đối với thực thể B.

3.13

Xác thực khóa tường minh của A đối với B (explicit key authentication from A to B)

Sự đảm bảo cho B rằng chỉ có A là thực thể sở hữu khóa đúng.

CHÚ THÍCH: Việc kết hợp giữa xác thực khóa ẩn của A đối với B và xác nhận khóa của A đối với B sẽ đảm bảo tính xác thực khóa tường minh của A đối với B.

3.14

Xác thực khóa ẩn của A đối với B (implicit key authentication from A to B)

Sự đảm bảo cho B rằng chỉ có A là thực thể có khả năng sở hữu khóa đúng.

3.15

Khóa (key)

Một dãy ký tự điều khiển hoạt động của phép biến đổi mật mã (ví dụ mã hóa, giải mã, tính hàm kiểm tra mật mã, tạo hoặc kiểm tra chữ ký số) [TCVN 7817-1 : 2007 (ISO/IEC 11770-1:1999)].

3.16

Thỏa thuận khóa (key agreement)

Tiến trình kiến tạo một khóa bí mật dùng chung giữa hai thực thể theo cách mà không có bên nào có thể định trước được giá trị cho khóa.

3.17

Xác nhận khóa của A đối với B (key confirmation from A to B)

Sự đảm bảo đối với thực thể B rằng thực thể A sở hữu một khóa đúng.

3.18

Kiểm soát khóa (key control)

Khả năng lựa chọn khóa hoặc tham số sử dụng trong một phép tính toán khóa.

3.19

Thiết lập khóa (key establishment)

Quá trình tạo nên sự khả dụng một khóa bí mật dùng chung cho một hoặc nhiều thực thể. Thiết lập khóa bao gồm thỏa thuận khóa và vận chuyển khóa.

3.20

Thẻ khóa (key token)

Thông điệp quản lý khóa gửi từ một thực thể đến một thực thể khác trong quá trình thực hiện một cơ chế quản lý khóa.

3.21

Vận chuyển khóa (key transport)

Tiến trình truyền một khóa từ một thực thể đến một thực thể khác với sự bảo vệ thích hợp.

3.22

Xác thực thực thể lẫn nhau (mutual entity authentication)

Sự xác thực giữa hai thực thể để đảm bảo về định danh của mỗi thực thể.

3.23

Hàm một chiều (one-way function)

Hàm có tính chất dễ dàng tính được đầu ra đối với đầu vào cho trước nhưng lại không thể tìm được đầu vào tương ứng nếu cho trước đầu ra.

3.24

Khóa riêng (private key)

Khóa thuộc một cặp khóa phi đối xứng của một thực thể chỉ được sử dụng bởi thực thể đó.

CHÚ THÍCH: Trong hệ thống chữ ký phi đối xứng, khóa riêng xác định phép biến đổi ký. Trong hệ mật phi đối xứng, khóa riêng xác định phép biến đổi giải mã.

3.25

Khóa công khai (public key)

Thành phần khóa thuộc cặp khóa phi đối xứng của một thực thể được công bố công khai.

CHÚ THÍCH: Trong hệ chữ ký phi đối xứng, khóa công khai xác định phép biến đổi kiểm tra chữ ký. Trong hệ mật phi đối xứng, khóa công khai xác định phép biến đổi mã hóa. Một khóa "được biết một cách công khai" không nhất thiết phải luôn khả dụng cho mọi đối tượng. Khóa đó có thể chỉ khả dụng đối với tất cả thành viên thuộc một nhóm định trước.

3.26

Chứng chỉ khóa công khai (public key certificate)

Thông tin khóa công khai của một thực thể được ký bởi Tổ chức chứng thực vì thế không thể giả mạo.

3.27

Thông tin khóa công khai (public key information)

Thông tin chứa ít nhất định danh phân biệt và khóa công khai của một thực thể. Thông tin khóa công khai được giới hạn bằng dữ liệu liên quan đến một thực thể và khóa công khai của thực thể đó. Ngoài ra, thông tin khóa công khai có thể bao gồm các thông tin tĩnh khác như cơ quan chứng thực, thực thể, khóa công khai, các giới hạn sử dụng khóa, thời gian hiệu lực hoặc thuật toán được sử dụng.

3.28

Khóa bí mật (secrect key)

Khóa sử dụng trong kỹ thuật mật mã đối xứng bởi một tập thực thể xác định.

3.29

Số tuần tự (sequence number)

Một tham số biến thiên theo thời gian có giá trị nhận từ một dãy xác định sao cho không có sự lặp lại trong một khoảng thời gian nhất định [TCVN 7817-1 : 2007(ISO/IEC 11770-1:1999)].

3.30

Hệ chữ ký (signature system)

Hệ thống dựa trên kỹ thuật mật mã phi đối xứng trong đó một phép biến đổi bí mật được dùng để ký và một phép biến đổi công khai được dùng để xác minh.

3.31

Tem thời gian (time stamp)

Một mục dữ liệu đánh dấu một thời điểm dùng để tham chiếu về mặt thời gian.

3.32

Tổ chức cung cấp tem thời gian (time stamping authority)

Bên thứ ba tin cậy được tin tưởng trong việc cung cấp bằng chứng bao gồm thời điểm mà tại đó tem thời gian an toàn được tạo ra [ISO/IEC 13888-1:1997].

3.33

Tham số biến thời gian (time variant parameter)

Một mục dữ liệu sử dụng để xác nhận rằng một thông điệp là không được sử dụng lại. Tham số biến thiên theo thời gian có thể là một số ngẫu nhiên, một số tuần tự hoặc một tem thời gian.

3.34

Bên thứ ba tin cậy (trusted third party)

Một tổ chức có thẩm quyền về an toàn, hoặc đại diện đủ tư cách của cơ quan đó, được tin cậy bởi các thực thể khác về khía cạnh hoạt động liên quan đến an toàn [ISO/IEC 10181-1:1996].

4 Ký hiệu và từ viết tắt

Tiêu chuẩn này sử dụng các ký hiệu và từ viết tắt sau đây :

A, B Các thẻ định danh riêng biệt của các thực thể *A* và thực thể *B*.

BE Khối dữ liệu được mã hóa.

BS Khối dữ liệu được ký.

CA Cơ quan chứng thực.

$Cert_A$ Chứng chỉ khóa công khai của thực thể *A*.

D_A Phép giải mã bằng khóa riêng của thực thể *A*.

d_A Khóa giải mã bí mật của thực thể *A*.

E_A Phép mã hóa công khai của thực thể *A*.

e_A Khóa mã công khai của thực thể *A*.

$F(h,g)$ Hàm thỏa thuận khóa.

f Hàm kiểm tra mật mã.

$f_K(Z)$ Giá trị kiểm tra mật mã, là kết quả thu được từ việc áp dụng hàm kiểm tra mật mã f khi sử dụng đầu vào là một khóa bí mật K và chuỗi dữ liệu tùy ý Z.

g Một phần tử chung được chia sẻ công khai giữa tất cả các thực thể cùng sử dụng một hàm thỏa thuận khóa F.

h_A Khóa riêng của thực thể A dùng để thỏa thuận khóa.

hash Hàm băm.

H Tập các phần tử.

G Tập các phần tử.

K Một khóa bí mật dùng cho hệ mật đối xứng.

K_{AB} Khóa bí mật dùng chung giữa hai thực thể A và B.

CHÚ THÍCH: Khi thực thi trong thực tế, khóa bí mật dùng chung có thể là đối tượng cần được xử lý thêm trước khi sử dụng cho hệ mật đối xứng.

KT Thẻ khóa.

KT_{Ai} Thẻ khóa được gửi bởi thực thể A sau pha xử lý thứ i.

p_A Khóa dùng để thỏa thuận khóa công khai của thực thể A.

PKI_A Thông tin khóa công khai của thực thể A.

r Một số ngẫu nhiên được sinh ra theo một cơ chế nào đó.

r_A Một số ngẫu nhiên được cấp bởi thực thể *A* trong một cơ chế thỏa thuận khóa.

S_A Phép biến đổi ký sử dụng khóa bí mật của thực thể A

s_A Khóa bí mật của thực thể *A* được sử dụng để ký.

Texti Một trường dữ liệu tùy chọn được sử dụng trong phạm vi áp dụng của tiêu chuẩn này.

TVP Tham số biến đổi theo thời gian, ví dụ như một số ngẫu nhiên, tem thời gian hoặc một số tuần tự.

V_A Phép biến đổi kiểm tra công khai của thực thể *A*.

v_A Khóa kiểm tra công khai của thực thể *A*.

w Hàm một chiều.

$\sum$ Chữ ký số.

|| Phép nối hai phần tử dữ liệu với nhau.

CHÚ THÍCH:

1. Không có giả định nào được tạo ra đối với bản chất phép biến đổi ký. Đối với hệ chữ ký có khôi phục thông điệp thì $S_A(m)$ là ký hiệu của chính chữ ký $\sum$. Trong trường hợp hệ chữ ký kèm phụ lục thì $S_A(m)$ là ký hiệu là thông điệp *m* kèm theo chữ ký $\sum$.

2. Các khóa của một hệ mật phi đối xứng được ký hiệu bằng chữ thường (thể hiện chức năng của khóa đó) và được đánh chỉ số là định danh của thực thể sở hữu khóa, ví dụ khóa kiểm tra công khai của thực thể *A* được ký hiệu là V_A. Phép biến đổi tương ứng được ký hiệu bằng chữ hoa và được đánh chỉ số theo tên chủ sở hữu, ví dụ phép biến đổi để kiểm tra khóa công khai của thực thể *A* được ký hiệu là V_A.

5 Các yêu cầu

Giả sử rằng các thực thể đều biết được định danh được tuyên bố của thực thể khác. Có thể đạt được điều này bằng việc đưa các định danh vào thông tin trao đổi giữa hai thực thể, hoặc điều này là hiển nhiên trong ngữ cảnh sử dụng cơ chế. Kiểm tra một định danh có nghĩa là xác minh xem trường định

danh nhận được có phù hợp với một số giá trị đã biết (được tin cậy) hoặc sự mong đợi trước đó hay không.

Nếu một khóa công khai được đăng ký cho một thực thể thì thực thể đó sẽ tạo nên được sự tin tưởng rằng thực thể đã đăng ký khóa công khai đang sở hữu một khóa riêng tương ứng (xem phần đăng ký khóa ở Phần tiêu chuẩn tổng quát).

6 Thỏa thuận khóa bí mật

Thỏa thuận khóa là tiến trình thiết lập một khóa bí mật dùng chung giữa hai thực thể *A* và *B* bằng một phương pháp mà không ai trong số *A* hoặc *B* có thể định trước được giá trị cho khóa bí mật dùng chung này. Các cơ chế thoả thuận khóa có thể cung cấp tính xác thực khóa ẩn. Trong ngữ cảnh của việc thiết lập khóa, xác thực khóa ẩn có nghĩa là sau khi thực thi cơ chế chỉ có một thực thể đã được chỉ ra là có thể nắm giữ được khóa bí mật dùng chung hợp lệ.

Thỏa thuận khóa giữa hai thực thể *A* và *B* diễn ra trong một hoàn cảnh được chia sẻ bởi hai thực thể. Hoàn cảnh này bao gồm các đối tượng sau: một tập *G*, một tập *H* và một hàm *F*. Hàm *F* phải thỏa mãn các yêu cầu sau:

1. Hàm *F* nhận 2 đầu vào, một phần tử *h* thuộc tập *H* và một phần tử *g* thuộc *G* cho đầu ra là *y* thuộc *G*, sao cho $y = F(h,g)$.

2. *F* thỏa mãn điều kiện giao hoán: $F(h_A, F(h_B,g)) = F(h_B, F(h_A,g))$.

3. Không thể tìm được $F(h_1, F(h_2,g))$ từ $F(h_1,g)$, $F(h_2,g)$ và *g*. Tính chất này chỉ ra rằng $F(.,g)$ là hàm một chiều.

4. Các thực thể *A* và *B* chia sẻ một phần tử chung *g* thuộc *G*, phần tử này có thể được biết một cách công khai.

5. Các thực thể tham gia thiết lập này có thể tính các giá trị của hàm $F(h,g)$ và có thể sinh ra các phần tử ngẫu nhiên thuộc *H* một cách hiệu quả.

Tùy thuộc vào từng cơ chế thỏa thuận khóa cụ thể mà có thể có thêm một số điều kiện khác.

CHÚ THÍCH:

1. Ví dụ về hàm *F* được đưa ra ở Phụ lục B.

2. Trong các cài đặt thực tế về các cơ chế thỏa thuận khóa, khóa bí mật dùng chung có thể là đối tượng phải xử lý thêm. Một khóa bí mật dùng chung dẫn xuất có thể được tính theo (1) bằng cách trích trực tiếp ra các bít từ một khóa bí mật dùng chung K_{AB} một cách trực tiếp, hoặc theo (2) bằng cách truyền một khóa bí mật dùng chung K_{AB} và dữ liệu không bí mật tùy chọn khác thông qua một hàm một chiều và trích ra các bít từ đầu ra.

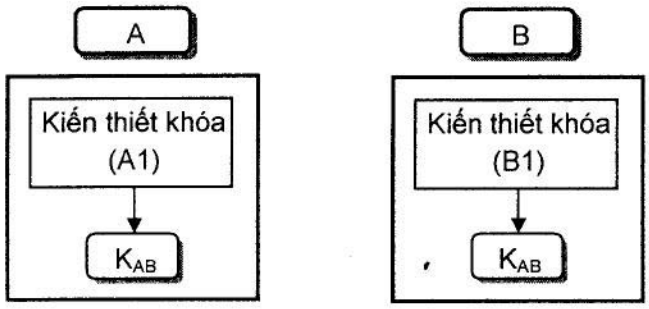
3. Thông thường sẽ cần phải kiểm tra giá trị hàm nhận được $F(h,g)$ đối với các giá trị yếu. Nếu phát hiện ra các giá trị yếu thì giao thức sẽ bị dừng lại. Một ví dụ điển hình là cơ chế thỏa thuận khóa Diffie-Hellman ở điều B.5 của Phụ lục B.

6.1 Cơ chế thỏa thuận khóa 1

Cơ chế thỏa thuận khóa này không tương tác dùng để thiết lập một khóa bí mật dùng chung giữa hai thực thể *A* và *B* có sự xác thực khóa ẩn lẫn nhau. Các yêu cầu sau phải được thỏa mãn:

1. Mỗi thực thể *X* có một khoá riêng dùng để thoả thuận khoá là h_X thuộc *H* và một khóa công khai dùng để thỏa thuận khoá $p_X = F(h_X,g)$.

2. Mỗi thực thể có khả năng truy cập được tới bản sao có xác thực của khoá công khai dùng để thỏa thuận khóa của thực thể kia. Điều kiện này có thể đạt được bằng việc sử dụng cơ chế ở điều 8.



Hình 1 – Cơ chế thỏa thuận khóa 1

Kiến thiết khoá (A1): *A* sử dụng khóa riêng dùng để thỏa thuận khóa h_A của mình và khóa công khai dùng để thỏa thuận khóa p_B của *B* để tính ra khóa bí mật dùng chung:

$$K_{AB} = F(h_A,p_B)$$

Kiến thiết khoá (B1): *B* sử dụng khóa riêng dùng để thỏa thuận khóa h_B của mình và khóa công khai dùng để thỏa thuận khóa p_A của *A* để tính toán ra khoá bí mật chia sẻ:

$$K_{AB} = F(h_B,p_A)$$

Như một hệ quả của yêu cầu 2 đối với hàm *F*, hai giá trị đã được tính cho khoá K_{AB} là giống nhau.

CHÚ THÍCH: Cơ chế thỏa thuận khóa này có các tính chất sau:

1. Số lần truyền: 0. Như một hệ quả, khóa bí mật dùng chung luôn có cùng một giá trị (xem thêm chú thích 2 mục 6).

2. Xác thực khóa: Cơ chế này cung cấp tính xác thực khóa ẩn lẫn nhau.

3. Xác nhận khóa: Cơ chế này không cung cấp khả năng xác nhận khóa.

4. Đây là một cơ chế thỏa thuận khóa vì khóa được thiết lập là hàm một chiều của các khoá dùng để thoả thuận khoá bí mật h_A của thực thể A và h_B của thực thể B. Tuy nhiên, một thực thể có thể biết được khóa công khai của thực thể kia trước khi chọn khóa bí mật cho cả hai. Để thực hiện được điều này, trong khoảng thời gian tìm ra khóa công khai của thực thể kia và chọn khóa bí mật cho cả hai, một thực thể có thể chọn ra xấp xỉ s bít từ khóa đã thiết lập, với chi phí 2^s giá trị có thể, sử dụng cho khóa dùng để thỏa thuận khóa bí mật dùng chung.

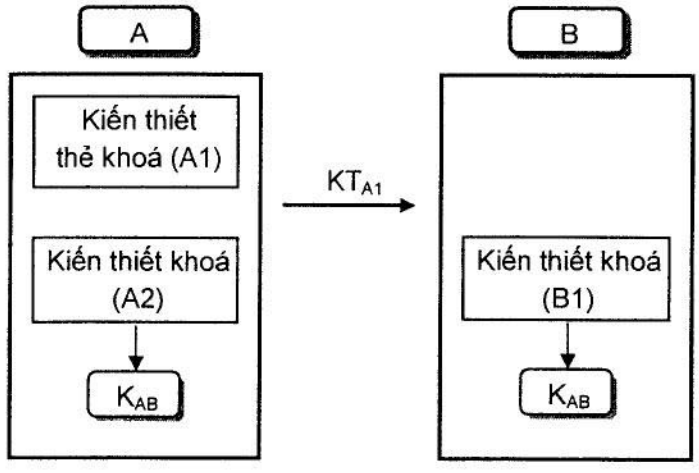
5. Ví dụ: Cơ chế thỏa thuận khóa Diffie-Hellman được đưa ra ở điều B.5.

6.2 Cơ chế thỏa thuận khóa 2

Cơ chế thỏa thuận khóa này thiết lập một khóa bí mật dùng chung giữa 2 thực thể A và B chỉ trong một lần truyền, có cung cấp tính xác thực khóa ẩn của B đối với A nhưng không cung cấp tính xác thực thực thể của A đối với B (B không biết đang thiết lập khóa bí mật dùng chung với ai). Trong cơ chế thỏa thuận khóa này, các yêu cầu sau cần phải được thỏa mãn:

1. Thực thể B có một khóa riêng dùng để thỏa thuận khóa là h_B thuộc H và một khóa công khai dùng để thỏa thuận khóa là $p_B = F(h_B,g)$.

2. Thực thể A có khả năng truy cập được tới bản sao có xác thực của khoá công khai dùng để thỏa thuận khóa p_B của B. Điều đạt được nhờ sử dụng cơ chế ở điều 8.



Hình 2 – Cơ chế thỏa thuận khóa 2

Kiến thiết thẻ khoá (A1): Trước tiên, *A* sinh ngẫu nhiên và bí mật giá trị *r* thuộc *H*, tính *F(r,g)* và gửi thẻ khoá KT_{A1} tới *B*:

$$KT_{A1} = F(r,g) \,||\, Text$$

Kiến thiết khoá (A2): Tiếp đó, *A* tính khóa bí mật dùng chung cho mình như sau:

$$K_{AB} = F(r,p_B)$$

Kiến thiết khoá (B1): *B* trích giá trị *F(r,g)* từ thẻ khoá KT_{A1} vừa nhận được và tính khóa bí mật dùng chung như sau:

$$K_{AB} = F(h_B,F(r,g))$$

Theo yêu cầu 2 của hàm *F* thì kết quả của hai giá trị tính toán tạo ra K_{AB} ở trên là giống nhau.

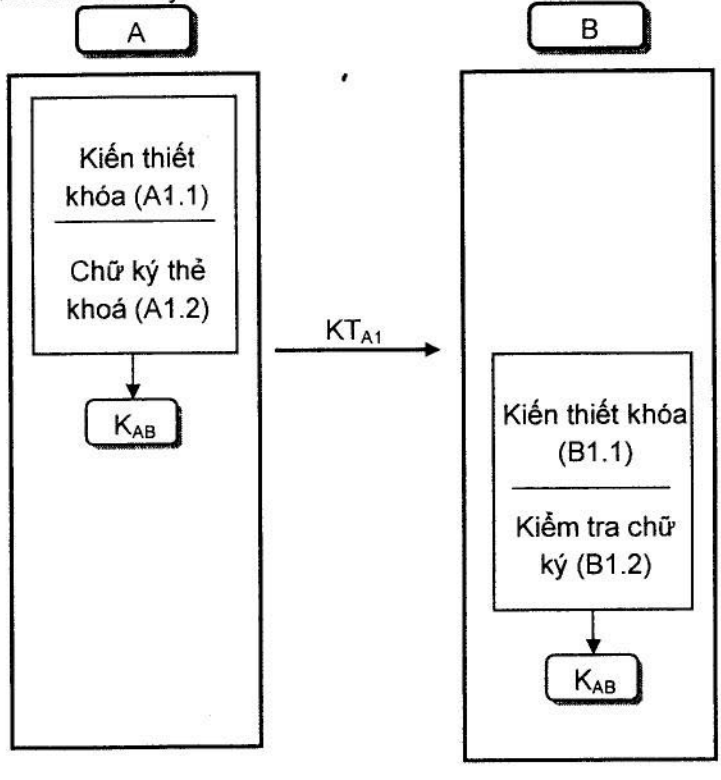
CHÚ THÍCH: Cơ chế thỏa thuận khóa này có các tính chất sau:

1. Số lần chuyển: 1.
2. Xác thực khoá: Cơ chế này cung cấp tính xác thực khóa ẩn của *B* đối với *A* (*B* là thực thể duy nhất ngoài *A* có thể tính được khóa bí mật dùng chung).
3. Xác nhận khóa: Cơ chế này không cung cấp tính xác nhận khóa.
4. Đây là một cơ chế thỏa thuận khóa vì khóa được thiết lập là hàm một chiều của giá trị ngẫu nhiên *r* cung cấp bởi *A* và khoá dùng để thoả thuận khoá bí mật của *B*. Tuy nhiên, do thực thể *A* có thể biết được khóa công khai của thực thể *B* trước khi chọn giá trị *r* nên *A* có thể chọn ra xấp xỉ *s* bít từ khóa đã thiết lập với chi phí 2^s giá trị có thể trong khoảng thời gian tìm ra khóa công khai của *B* và gửi KT_{A1}.
5. Ví dụ: Một ví dụ cho cơ chế thỏa thuận khóa này là cơ chế thỏa thuận khóa ElGamal mô tả ở điều B.3.
6. Sử dụng khóa: Do *B* nhận khóa K_{AB} từ thực thể không được xác thực *A* nên việc sử dụng an toàn K_{AB} ở đầu cuối *B* được giới hạn trong các chức năng không đòi hỏi tính tin cậy trong tính chất xác thực của *A* chẳng hạn như giải mã và tạo các mã xác thực thông điệp.

6.3 Cơ chế thỏa thuận khóa 3

Cơ chế thỏa thuận khóa này thiết lập một khóa bí mật dùng chung giữa 2 thực thể *A* và *B* bằng một lần truyền, cung cấp tính chất xác thực khóa ẩn lẫn nhau và xác thực thực thể của *A* đối với *B*. Đối với cơ chế này, các yêu cầu sau phải được thỏa mãn:

1. Thực thể *A* có một hệ chữ ký phi đối xứng (S_A, V_A).
2. Thực thể *B* phải truy cập được tới bản sao có xác thực của phép kiểm tra công khai V_A.
3. Thực thể *B* có một hệ thoả thuận khoá (h_B, p_B).
4. Thực thể *A* có khả năng truy cập được đến một bản sao khóa thỏa thuận khóa công khai có xác thực p_B của thực thể *B*. Điều kiện này được thỏa mãn nhờ sử dụng cơ chế ở mục 8.
5. *TVP*: *TVP* có thể là một tem thời gian hoặc là số tuần tự. Nếu tem thời gian được sử dụng thì cần có sự an toàn và đồng bộ về mặt thời gian. Nếu số tuần tự được sử dụng thì cần có khả năng duy trì và kiểm tra các bộ đếm của 2 bên.
6. Cả thực thể *A* và thực thể *B* thỏa thuận với nhau cùng sử dụng một hàm kiểm tra mật mã *f* (chẳng hạn như các hàm được quy định trong ISO/IEC 9797) và một cách kết hợp K_{AB} như là khoá trong hàm kiểm tra này.



Hình 3 – Cơ chế thỏa thuận khóa 3

Kiến thiết khoá (A1.1): Trước hết, thực thể *A* sinh ngẫu nhiên và bí mật *r* thuộc *H* và tính *F(r,g)*. Tiếp đó, *A* tính khóa bí mật dùng chung như sau:

$K_{AB} = F(r,p_B)$ Sử dụng khóa bí mật dùng chung K_{AB}, *A* tính giá trị kiểm tra mật mã dựa trên phép nối định danh phân biệt của người gửi *A* và số tuần tự hoặc tem thời gian *TVP*.

Chữ ký thẻ khoá (A1.2): *A* thực hiện ký giá trị kiểm tra mật mã sử dụng phép biến đổi chữ ký bí mật S_A của mình. Sau đó *A* tạo thẻ khoá KT_{A1}, bao gồm định danh phân biệt của người gửi *A*, đầu vào khoá *F(r, g)*, *TVP*, giá trị kiểm tra mật mã đã được ký và dữ liệu tuỳ chọn nào đó rồi gửi tới *B*:

$$KT_{A1} = A \,||\, F(r,g) \,||\, TVP \,||$$

$$S_A\,(f_{KAB}(ID_A \,||\, TVP)) \,||\, Text1$$

Kiến thiết khoá (B1.1): Thực thể *B* trích giá trị *F(r,g)* từ thẻ khoá nhận được KT_{A1} và tính khóa bí mật dùng chung bằng cách sử dụng khóa riêng dùng để thỏa thuận khóa h_B như sau:

$$K_{AB} = F(h_B,F(r,g))$$

Sử dụng khóa bí mật dùng chung K_{AB} B để tính giá trị kiểm tra mật mã trên định danh phân biệt của người gửi *A* và *TVP*.

Kiểm tra chữ ký (B1.2): Thực thể *B* sử dụng phép kiểm tra công khai V_A để kiểm tra chữ ký của *A* bằng hàm V_A, kiểm tra tính toàn vẹn cùng và nguồn gốc của thẻ khoá đã nhận được KT_{A1}. Sau đó, *B* xác nhận tính phụ thuộc vào thời gian của thẻ (bằng cách xem xét *TVP*).

CHÚ THÍCH : Cơ chế thỏa thuận khóa này có một số tính chất sau :

1. Số lần chuyển: 1.
2. Xác thực khóa : Cơ chế này cung cấp tính xác thực khóa hiện của *A* đối với *B* và tính xác thực khóa ẩn của *B* đối với *A*.
3. Xác nhận khóa: Cơ chế này cung cấp tính xác nhận khóa của *A* đối với *B*.
4. Đây là cơ chế thỏa thuận khóa vì khóa được thiết lập là hàm một chiều của giá trị ngẫu nhiên *r* được cung cấp bởi *A* và khóa riêng dùng để thỏa thuận khóa của *B*. Tuy nhiên, do thực thể *A* có thể biết được khóa công khai của thực thể *B* trước khi *A* chọn giá trị ngẫu nhiên *r* nên thực thể *A* có thể chọn trước

khoảng *s* bit của khoá được thiết lập với chi phí phải sinh khoảng 2^s giá trị có thể cho *r* trong khoảng thời gian tìm ra khóa công khai của thực thể *B* và gửi KT_{A1}.

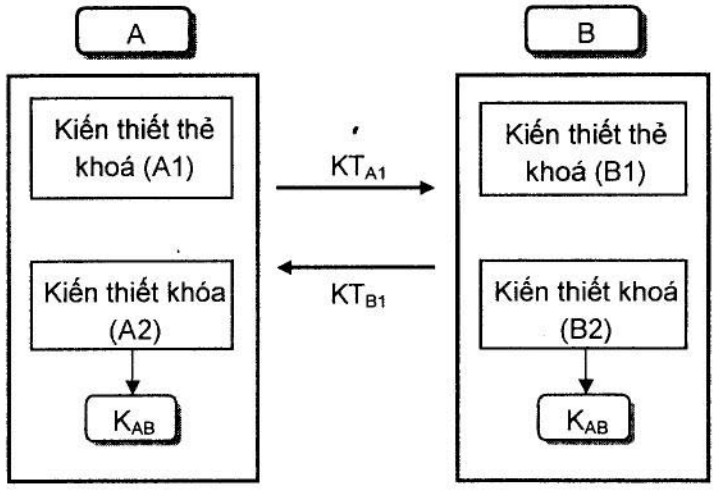
5. *TVP*: cung cấp Sự xác thực thực thể của *A* đối với *B* và ngăn ngừa việc dùng lại thẻ khóa..

6. Ví dụ: Một ví dụ về cơ chế thỏa thuận khóa dạng này là thỏa thuận khóa Nyberg-Rueppel mô tả ở điều *B*.4.

7. Chứng chỉ khóa công khai: Nếu trường *Text1* được sử dụng để truyền chứng khóa công khai của *A* thì yêu cầu thứ 2 tại phần đầu của mục này có thể được nới nhẹ rằng đòi hỏi *B* phải nắm giữ bản sao có xác thực của khoá kiểm tra công khai của CA.

6.4 Cơ chế thỏa thuận khóa 4

Cơ chế thỏa thuận khóa này thiết lập một khóa bí mật dùng chung giữa 2 thực thể *A* và *B* trong hai lần chuyển, kết hợp với việc kiểm soát khóa không có sự trao đổi trước thông tin về khóa. Cơ chế này không cung cấp tính xác thực khóa và xác thực thực thể.



Hình 4 – Cơ chế thỏa thuận khóa 4

Kiến thiết thẻ khoá (A1): Thực thể sinh ra ngẫu nhiên và bí mật r_A thuộc *H*, tính $F(r_A,g)$, tạo thẻ khóa KT_{A1} và gửi tới *B*:

$$KT_{A1} = F(r_A,g) \,||\, Text1$$

Kiến thiết thẻ khoá (B1): Thực thể *B* sinh ngẫu nhiên và bí mật r_B thuộc *H*, tính $F(r_B,g)$, kiến thiết thẻ khóa KT_{B1} và gửi tới *A*:

$$KT_{B1} = F(r_B,g) \,||\, Text2$$

Kiến thiết khoá (A2): Thực thể *A* trích giá trị $F(r_B,g)$ từ thẻ khoá nhận được KT_{B1} và tính khóa bí mật dùng chung như sau:

$$K_{AB} = F(r_A,F(r_B,g))$$

Kiến thiết khoá (B2): Thực thể *B* trích giá trị $F(r_A,g)$ từ thẻ khoá nhận được KT_{A1} và tính khóa bí mật dùng chung như sau:

$$K_{AB} = F(r_B,F(r_A,g))$$

CHÚ THÍCH: Cơ chế thỏa thuận khóa này có các tính chất sau:

1. Số lần chuyển: 2.
2. Xác thực khóa: Cơ chế này không cung cấp tính xác thực khóa. Tuy nhiên, cơ chế này có thể hữu dụng trong các môi trường mà ở đó tính xác thực của thẻ khóa được kiểm tra bằng một phương pháp khác. Chẳng hạn, một mã băm của các thẻ khoá có thể được trao đổi giữa các thực thể bằng cách sử dụng một kênh truyền thông thứ hai. Xem thêm phần Cơ chế vận chuyển khóa công khai 2.
3. Xác nhận khóa: Cơ chế này không cung cấp tính xác nhận khóa.
4. Đây là một cơ chế thỏa thuận khóa vì khóa được thiết lập là hàm một chiều của các giá trị ngẫu nhiên r_A cung cấp tương ứng bởi *A* và r_B được cung cấp bởi *B*. Tuy nhiên, do thực thể *B* có thể biết được $F(r_A,g)$ trước khi *B* chọn giá trị ngẫu nhiên r_B nên *B* có thể chọn trước khoảng *s* bit trong giá trị khóa đã thiết lập với chi phí khoảng 2^s giá trị có thể cho r_B trong khoảng thời gian nhận KT_{A1} và gửi KT_{B1}.
5. Ví dụ: Một ví dụ về cơ chế thỏa thuận khóa dạng này là thỏa thuận khóa Diffie-Hellman trình bày ở phụ lục *B*.5.

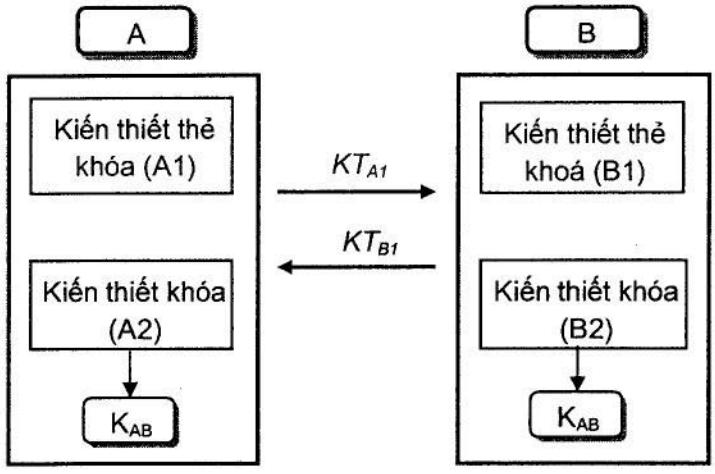
6.5 Cơ chế thỏa thuận khóa 5

Cơ chế thỏa thuận khóa này thiết lập một khóa bí mật dùng chung giữa 2 thực thể *A* và *B* trong hai lần truyền có sự xác thực khóa ẩn lẫn nhau và cùng kiểm soát khóa. Trong có chế này, các yêu cầu sau phải thỏa mãn:

1. Thực thể X có một khóa riêng dùng để thỏa thuận khóa là h_X thuộc H và một khóa công khai dùng để thỏa thuận khóa là $p_X = F(h_X,g)$.

2. Mỗi thực thể có khả năng truy cập được đến bản sao khóa công khai dùng để thỏa thuận khóa có xác thực của thực thể kia. Điều kiện này có thể đạt được nhờ sử dụng cơ chế ở điều 8.

3. Cả hai thực thể thỏa thuận cùng sử dụng hàm một chiều w.



Hình 5 – Cơ chế thỏa thuận khóa 5

Kiến thiết thẻ khoá (A1): Thực thể A sinh ngẫu nhiên và bí mật r_A thuộc H, tính $F(r_A,g)$, tạo thẻ khóa KT_{A1} và gửi tới B:

$$KT_{A1} = F(r_A,g) \,||\, Text1$$

Kiến thiết thẻ khoá (B1): Thực thể B sinh ngẫu nhiên và bí mật r_B thuộc H, tính $F(r_B,g)$, tạo thẻ khóa KT_{B1} và gửi tới A:

$$KT_{B1} = F(r_B,g) \,||\, Text2$$

Kiến thiết khoá (B2): Thực thể B trích lấy giá trị $F(r_A,g)$ trong thẻ khoá KT_{A1} nhận được rồi tính khóa bí mật dùng chung như sau:

$$K_{AB} = w(F(r_B,F(r_A,g)),F(r_B,p_A))$$

Kiến thiết khoá (A2): Thực thể *A* trích lấy giá trị $F(r_B,g)$ trong thẻ khoá KT_{B1} nhận được rồi tính khóa bí mật dùng chung như sau:

$$K_{AB} = w(F(r_A,F(r_B,g)),F(r_A,p_B))$$

CHÚ THÍCH: Cơ chế thỏa thuận khóa này có các tính chất sau đây:

1. Số lần chuyển: 2.

2. Xác thực khóa: Cơ chế này có cung cấp tính xác thực khóa ẩn lẫn nhau. Nếu trường dữ liệu *Text2* chứa giá trị kiểm tra mật mã (trên dữ liệu đã biết) được tính bằng cách sử dụng khóa K_{AB} thì cơ chế này cung cấp tính xác thực khóa tường minh của *B* đối với *A*.

3. Xác nhận khóa: Nếu trường dữ liệu *Text2* chứa giá trị kiểm tra mật mã (trên dữ liệu đã biết) được tính bằng cách sử dụng khóa K_{AB} thì cơ chế trao đổi khóa này cung cấp tính xác nhận khóa của *B* đối với *A*.

4. Đây là một cơ chế thỏa thuận khóa vì khóa được thiết lập là hàm một chiều của các giá trị ngẫu nhiên r_A cung cấp tương ứng bởi *A* và r_B cung cấp bởi *B*. Tuy nhiên, do thực thể *B* có thể biết được $F(r_A,g)$ trước khi *B* chọn giá trị ngẫu nhiên r_B nên *B* có thể chọn trước khoảng *s* bit trong giá trị khóa đã thỏa thuận với chi phí khoảng 2^s giá trị có thể cho r_B trong khoảng thời gian nhận KT_{A1} và gửi KT_{B1}.

5. Ví dụ: Một ví dụ về cơ chế thỏa thuận khóa dạng này là cơ chế thỏa thuận khóa Matsumoto-Takashima-Imai A(0) sẽ được nói đến ở Phụ lục B.6. Một ví dụ khác là giao thức Goss.

6. Hàm *w* che giấu các đầu vào của nó theo chiều hướng từ giá trị của hàm và một trong các giá trị đầu vào sao cho không thể tính toán được các thành phần đầu vào liên quan khác. Điều này có thể thực hiện nhờ sử dụng hàm băm mô tả trong ISO/IEC 10118 (tuy nhiên không cần đến hàm băm kháng va chạm).

7. Các chứng chỉ khoá công khai: Nếu *Text1* và *Text2* chứa các chứng chỉ khoá công khai của các khoá thoả thuận khoá của thực thể *A* và *B* tương ứng thì yêu cầu 2 ở phần đầu của điều này có thể được thay bằng yêu cầu rằng mỗi thực thể phải nắm giữ được bản sao có xác thực của khoá kiểm tra công khai của CA.

6.6 Cơ chế thỏa thuận khóa 6

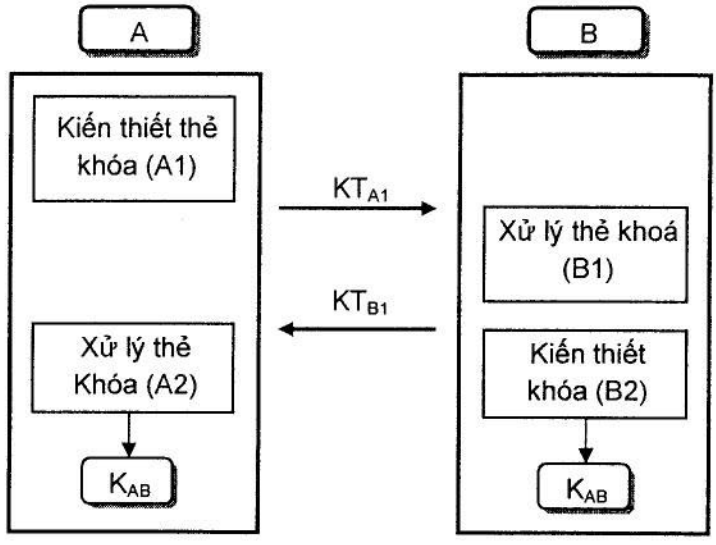
Cơ chế thỏa thuận khóa này thiết lập một khóa bí mật dùng chung giữa thực thể *A* và thực thể *B* trong 2 lần truyền, có cung cấp tính xác thực khóa ẩn lẫn nhau và kiểm soát khóa chung. Cơ chế này sử dụng một hệ thống gồm một hệ mật phi đối xứng và một hệ chữ ký. Các yêu cầu sau cần phải thỏa mãn:

1. Thực thể *A* có một hệ mật phi đối xứng với các biến đổi (E_A,D_A).

2. Thực thể *B* có một hệ chữ ký phi đối xứng với các biến đổi (S_B,V_B).

3. Thực thể *A* truy cập được tới bản sao có xác thực của phép kiểm tra công khai V_B của *B*. Điều kiện này có thể được thỏa mãn nhờ sử dụng cơ chế ở điều 8.

4. Thực thể *B* truy cập được tới bản sao có xác thực của phép mã hóa hoá công khai E_A của *A*. Điều kiện này có thể thực hiện được nhờ các cơ chế ở điều 8.



Hình 6 – Cơ chế trao đổi khóa 6

Kiến thiết thẻ khoá (A1): Thực thể *A* sinh ngẫu nhiên và bí mật r_A, tính toàn thẻ khóa KT_{A1} rồi gửi tới thực thể *B*:

$$KT_{A1} = r_A \,||\, Text1$$

Xử lý thẻ khoá (B1): Thực thể *B* sinh ngẫu nhiên và bí mật r_B, thực hiện ký khối dữ liệu gồm định danh phân biệt của *A*, số ngẫu nhiên r_A, số ngẫu nhiên r_B và một vài dữ liệu tùy chọn *Text2* bằng cách sử dụng phép biến đổi ký bí mật S_B của mình:

$$BS = S_B(A \,||\, r_A \,||\, r_B \,||\, Text2)$$

Tiếp đó, *B* mã hóa khối dữ liệu gồm định danh phân biệt của *B* (tùy chọn), khối đã được ký *BS* và một vài dữ liệu tùy chọn *Text3* bằng cách sử dụng phép mã hóa hóa công khai E_A của *A* và gửi thẻ khoá KT_{B1} thu được ngược trở lại cho *A*:

$$KT_{B1} = E_A(B \,||\, BS \,||\, Text3) \,||\, Text4$$

Kiến thiết khoá (B2): Khóa bí mật dùng chung bao gồm tất cả hoặc một phần chữ ký Σ của *B* được chứa trong khối đã ký *BS* (xem Chú thích 1 của Mục 4).

Xử lý thẻ khoá (A2): Thực thể *A* sử dụng phép biến đổi giải mã bí mật D_A của mình để giải mã thẻ khoá KT_{B1}, tiếp đến kiểm tra định danh của người gửi *B* theo tùy chọn rồi sử dụng phép kiểm tra công khai V_B của *B* để kiểm tra chữ ký số của khối đã được ký *BS*. Tiếp nữa, *A* kiểm tra định danh người nhận *A* và tính vững chắc của số ngẫu nhiên r_A trong khối đã ký *BS* rồi đem so với số ngẫu nhiên r_A được gửi đến trong thẻ KT_{A1}. Nếu tất cả quá trình kiểm tra thành công thì thực thể *A* chấp nhận tất cả hoặc một phần chữ ký Σ của *B* thuộc khối đã ký *BS* như là khoá bí mật dùng chung.

CHÚ THÍCH: Cơ chế thỏa thuận khóa này có một số tính chất sau:

1. Số lần chuyển: 2.

2. Xác thực khóa: Cơ chế này cung cấp tính xác thực khóa ẩn của *A* đối với *B* và xác thực khóa tường minh của *B* đối với *A*.

3. Xác nhận khóa: Nếu trường dữ liệu *Text3* chứa giá trị kiểm tra mật mã (trên dữ liệu đã biết) được tính toán bằng cách sử dụng khóa K_{AB} thì cơ chế trao đổi khóa này cung cấp tính xác nhận khóa của *B* đối với *A*.

4. Đây là một cơ chế thỏa thuận khóa vì khóa thiết lập là hàm một chiều của các giá trị ngẫu nhiên r_A của thực thể *A* và r_B của thực thể *B*. Tuy nhiên, do thực thể *B* có thể biết được $F(r_A,g)$ trước khi *B* chọn giá trị ngẫu nhiên r_B nên thực thể *B* có thể chọn trước xấp xỉ *s* bít trong giá trị khóa đã thiết lập với chi phí khoảng 2^s giá trị có thể cho r_B trong khoảng thời gian nhận KT_{A1} và gửi KT_{B1}.

5. Ví dụ: Một ví dụ về cơ chế thỏa thuận khóa dạng này là giao thức hai lần truyền của Beller và Yacobi sẽ được nói rõ ở Phụ lục B.7.

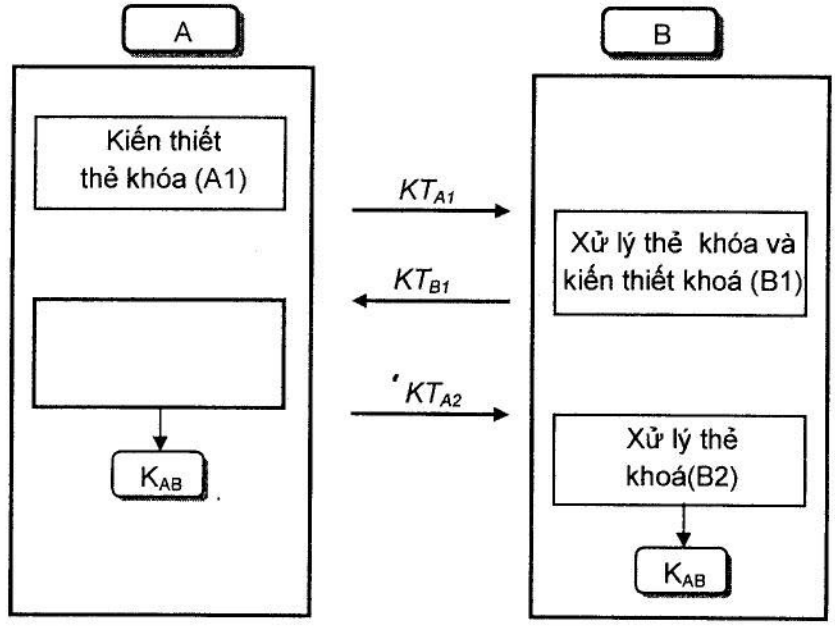
6. Chứng chỉ khóa công khai: Nếu trường *Text1* và *Text4* có chứa chứng chỉ khóa công khai dùng cho khóa mã của *A* và chứng chỉ khóa công khai dùng cho khóa kiểm tra của *B* thì yêu cầu thứ 3 và 4 ở cơ chế này có thể được giảm nhẹ thành một yêu cầu rằng mỗi thực thể phải có khả năng truy cập được đến bản sao có xác thực của khóa kiểm tra công khai cung cấp bởi CA.

7. Một đặc điểm quan trọng của cơ chế này là định danh của thực thể *B* có thể vẫn được giữ ở dạng nặc danh đối với các kẻ thu trộm, đây là ưu điểm rõ rệt trong môi trường mạng không dây – môi trường chính cho ứng dụng cơ chế này.

6.7 Cơ chế thỏa thuận khóa 7

Đây là cơ chế thỏa thuận khóa dựa trên cơ chế xác thực 3 lần truyền trong chuẩn ISO/IEC 9798-3. Cơ chế này thiết lập một khóa bí mật dùng chung giữa 2 thực thể *A* và *B* trong 3 lần truyền thông tin. Trong cơ chế này, một số yêu cầu sau cần được thỏa mãn:

1. Mỗi thực thể *X* sử dụng một hệ chữ ký (S_X, V_X).
2. Mỗi thực thể đều có khả năng truy cập đến bản sao có xác thực của phép kiểm tra công khai của thực thể kia. Điều kiện này có thể thực hiện nhờ các cơ chế ở điều 8.
3. Mỗi thực thể có một hàm kiểm tra mật mã chung *f*.



Hình 7 – Cơ chế trao đổi khóa 7

Kiến thiết thẻ khoá (A1): *A* sinh ra một giá trị ngẫu nhiên và bí mật r_A thuộc *H*, tính $F(r_A, g)$, kiến thiết thẻ khoá KT_{A1} và gửi nó tới *B:*

$$KT_{A1} = F_A(r_A, g) \,||\, Text1$$

Xử lý thẻ khoá và Kiến thiết khoá (B1): *B* sinh một giá trị ngẫu nhiên và bí mật r_B thuộc *H*, tiếp đó tính $F(r_B, g)$ rồi tính khóa bí mật dùng chung:

$$K_{AB} = F(r_B, F(r_A, g))$$

Tiếp theo, *B* tạo nên thẻ khoá được ký như sau:

$$KT_{B1} = S_B(DB_1) \,||\, f_{KAB}(DB_1) \,||\, Text\ 3$$

trong đó

$$DB_1 = F(r_B, g) \,||\, F(r_A, g) \,||\, A \,||\, Text\ 2$$

và gửi nó ngược trở lại *A*.

Tính xác nhận khóa được cung cấp bằng việc gửi $f_{KAB}(DB_1)$ trong thông báo KT_{B1}. Như một sự lựa chọn, nếu cả hai bên đều có một hệ mật đối xứng dùng chung thì sự xác nhận khóa có thể đạt được bởi thành phần mã hóa thẻ khóa như sau: thay thế KT_{B1} bởi $F(r_B, g) \,||\, E_{KAB}(S_B(DB_1))$.

Xử lý thẻ khoá (A2): Thực thể *A* kiểm tra chữ ký của *B* trên thẻ khoá KT_{B1} bằng cách sử dụng khóa kiểm tra công khai của *B*, kiểm tra định danh phân biệt của *A* và giá trị $F(r_A, g)$ đã được gửi ở bước (A1). Nếu quá trình kiểm tra thành công thì *A* sẽ tính khóa bí mật dùng chung là:

$$K_{AB} = F(r_A, F(r_B, g))$$

Thực thể *A* lại sử dụng khóa bí mật dùng chung K_{AB} để kiểm tra giá trị kiểm tra mật mã $f_{KAB}(DB_1)$. Sau đó *A* tạo một thẻ khoá được ký như sau:

$$KT_{A2} = S_A(DB_2) \,||\, f_{KAB}(DB_2) \,||\, Text5$$

trong đó

$$DB_2 = F(r_A, g) \,||\, F(r_B, g) \,||\, A \,||\, Text4$$

và gửi thẻ này tới thực thể *B*.

Tính xác nhận khóa cung cấp bằng việc gửi $f_{KAB}(DB_2)$ trong thông báo KT_{A2}. Như một sự lựa chọn, sự xác nhận khóa có thể đạt được bằng thành phần mã hóa thẻ khóa như sau: thay thế KT_{A2} bởi $F(r_B, g) \,||\, E_{KAB}(S_A(DB_2))$.

Xử lý thẻ khoá (B2): Thực thể *B* kiểm tra chữ ký của *A* trên thẻ khoá KT_{A2} sử dụng khóa kiểm tra công khai của *A*, sau đó nó kiểm tra định danh phân biệt của *B* và kiểm tra các giá trị $F(r_A, g)$ và $F(r_B, g)$ xem

có phù hợp với các giá trị được trao đổi ở các bước trước hay không. Nếu quá trình kiểm tra thành công thì *B* sẽ kiểm tra giá trị kiểm tra mật mã $f_{KAB}(DB_2)$ bằng cách tính:

$$K_{AB} = F(r_B, F(r_A, g))$$

CHÚ THÍCH: Cơ chế thỏa thuận khóa này có các tính chất sau:

1. Số lần chuyển: 3

2. Xác thực thực thể và xác thực khóa: Cơ chế này cung cấp tính xác thực khóa tường minh và xác thực thực thể lẫn nhau.

3. Xác nhận khóa: Cơ chế này cung cấp tính xác nhận khóa cho cả hai bên.

4. Đây là một cơ chế thỏa thuận khóa bởi vì khóa được thiết lập là hàm một chiều của các giá trị ngẫu nhiên r_A cung cấp bởi thực thể *A* và r_B được được cung cấp bởi thực thể *B*. Tuy nhiên, do thực thể *B* có thể biết giá trị $F(r_A,g)$ trước khi chọn giá trị r_B vì thế thực thể *B* có thể lựa chọn xấp xỉ *s* bit trong khóa đã thiết lập với chi phí khoảng 2^s giá trị có thể cho r_B trong khoảng thời gian từ khi *B* nhận KT_{A2} và gửi KT_{B1}.

5. Ví dụ: Một ví dụ về cơ chế thỏa thuận khóa dạng này là cơ chế Diffie-Hellman mô tả ở Phụ lục B và một cơ chế chữ ký số mô tả trong ISO/IEC 9796.

6. Phù hợp tiêu chuẩn: Cơ chế này phù hợp với ISO/IEC 9798-3, *Entity authentication using a public key algorithm (Xác thực thực thể sử dụng thuật toán khóa công khai)*. KT_{A1}, KT_{B1} và KT_{A2} là giống hệt nhau trong các thẻ gửi đến ở ba lần truyền của cơ chế xác thực mô tả ở mục 5.2.2 trong ISO/IEC 9798-3. Các trường dữ liệu cũng đồng nhất các thay đổi sau về việc sử dụng:

    a. Trường dữ liệu R_A (trình bày trong cả ba thẻ ở điều 5.2.2 của ISO/IEC 9798-3) biến đổi thành giá trị hàm ngẫu nhiên $F(r_B,g)$.

    b. Trường dữ liệu R_B (trình bày trong cả ba thẻ ở điều 5.2.2 của ISO/IEC 9798-3) biến đổi thành giá trị hàm ngẫu nhiên $F(r_B,g)$.

7. Chứng chỉ khóa công khai: Nếu trường dữ liệu *Text1* và *Text3* (hoặc *Text5* và *Text3*) chứa chứng chỉ số của thực thể *A* và *B* thì yêu cầu 2 của mục này có thể được giảm nhẹ và chỉ đòi hỏi rằng tất cả các thực thể phải có bản sao được xác thực khoá kiểm tra công khai cung cấp bởi CA.

8. Phép biến đổi ký: Nếu một cơ chế chữ ký số có băm văn bản thì $F(r_A,g)$ và/hoặc $F(r_B,g)$ không cần được gửi kèm trong thẻ khoá KT_{B1}. Tương tự, $F(r_A,g)$ và $F(r_B,g)$ cũng không được gửi kèm trong thẻ KT_{A2}. Tuy nhiên, phải đảm bảo rằng các số ngẫu nhiên phải được bao gồm trong quá trình tính toán chữ ký.

7 Vận chuyển khóa bí mật

Tiêu chuẩn này sẽ trình bày về các cơ chế vận chuyển một khóa bí mật được chọn bởi một thực thể (hoặc chọn bởi trung tâm tin cậy) cho một thực thể khác với sự bảo vệ thích hợp bằng kỹ thuật phi đối xứng.

CHÚ THÍCH: Trong thực tế thực thi các cơ chế vận chuyển khóa, một khối dữ liệu khóa có thể là đối tượng cần được xử lý trước khi tiến hành mã hóa. Chẳng hạn, một khối dữ liệu khóa có thể được áp dụng phép XOR với một mẫu bít (giả) ngẫu nhiên để hủy bỏ bất cứ cấu trúc bên ngoài nào của khối dữ liệu khóa.

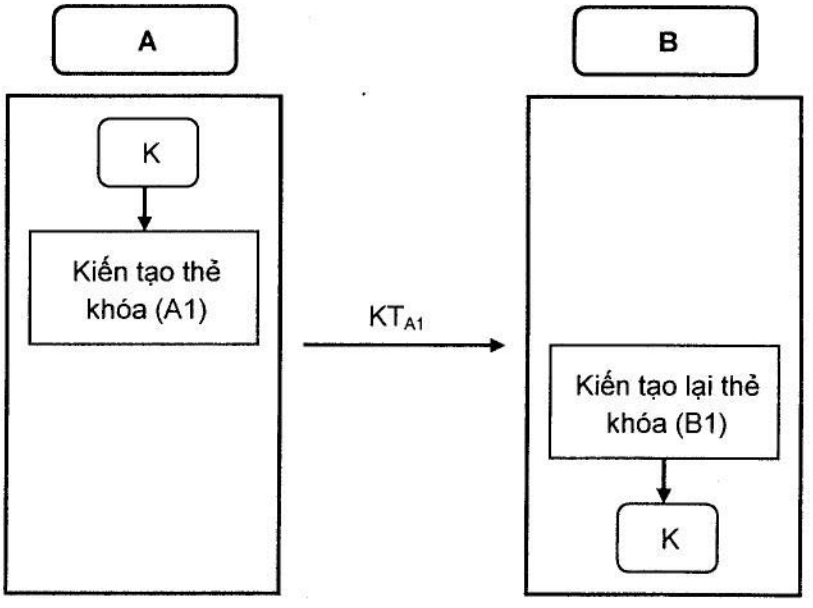
7.1 Cơ chế vận chuyển khóa 1

Cơ chế vận chuyển khóa này thực hiện truyền một lần một khóa bí mật từ thực thể *A* đến thực thể *B* có cung cấp tính xác thực khóa ẩn của *B* đối với *A*. Các yêu cầu sau cần được thỏa mãn:

1. Thực thể *B* có một hệ mật phi đối xứng (E_B, D_B).

2. Thực thể *A* có khả năng truy cập được đến bản sao có xác thực của phép mã hóa công khai của *B*. Điều kiện này có thể thực hiện được nhờ việc sử dụng các cơ chế ở mục 8.

3. Một giá trị *TVP* tùy ý có thể là một tem thời gian hoặc một số tuần tự được sử dụng. Nếu tem thời gian được sử dụng thì thực thể *A* và thực thể *B* cần duy trì sự đồng bộ về thời gian hoặc sử dụng một tem thời gian cung cấp bởi bên thứ ba tin cậy. Nếu số tuần tự được sử dụng thì *A* và *B* phải cùng duy trì một bộ đếm.



Hình 8 – Cơ chế vận chuyển khóa 1

Kiến thiết thẻ khóa (A1): *A* có một khóa *K* và muốn chuyển giao nó một cách an toàn đến *B*. Trước tiên, *A* kiến tạo một khối dữ liệu khóa bao gồm định danh riêng biệt của nó (không bắt buộc), khóa *K*, một giá trị *TVP* và trường dữ liệu tùy ý *Text1*. Tiếp đó *A* mã hóa khối dữ liệu khóa sử dụng phép mã hóa công khai của bên nhận E_B và gửi thẻ khóa sang cho *B*:

$$KT_{A1} = E_B(A \,||\, K \,||\, TVP \,||\, Text1) \,||\, Text\ 2$$

Kiến tạo lại thẻ khóa (B1): *B* nhận được thẻ khóa KT_{A1} sẽ tiến hành giải mã bằng cách sử dụng phép giải mã bí mật D_B của chính nó. Tiếp đó, phục hồi lại khóa *K*, kiểm tra giá trị *TVP* tùy ý và kết hợp khóa *K* phục hồi được với bên truyền *A*.

CHÚ THÍCH: Cơ chế vận chuyển khóa này có các tính chất sau:

1. Số lần truyền: 1
2. Xác thực khóa: Cơ chế này cung cấp việc xác thực khóa ẩn của *B* đối với *A* bởi vì chỉ có *B* mới có khả năng phục hồi lại khóa *K*.
3. Xác nhận khóa: Cơ chế này không cung cấp tính xác nhận khóa.
4. Kiểm soát khóa: *A* có thể lựa chọn khóa.
5. *TVP*: Một giá trị *TVP* tùy ý được sử dụng để ngăn ngừa việc dùng lại thẻ khóa.
6. Cách sử dụng khóa: Khi *B* nhận một khóa *K* từ một thực thể không được xác thực *A*, để sử dụng an toàn khóa K thì *B* sẽ hạn chế sử dụng cho các hàm không yêu cầu phải xác thực *A* như hàm giải mã và hàm tạo các mã xác thực thông điệp.
7. Ví dụ: Một ví dụ về cơ chế vận chuyển khóa dạng này là vận chuyển khóa ElGamal sẽ được mô tả ở điều B.8. Một ví dụ khác là cơ chế vận chuyển khóa RSA sẽ được mô tả ở điều B.10.

7.2 Cơ chế vận chuyển khóa 2

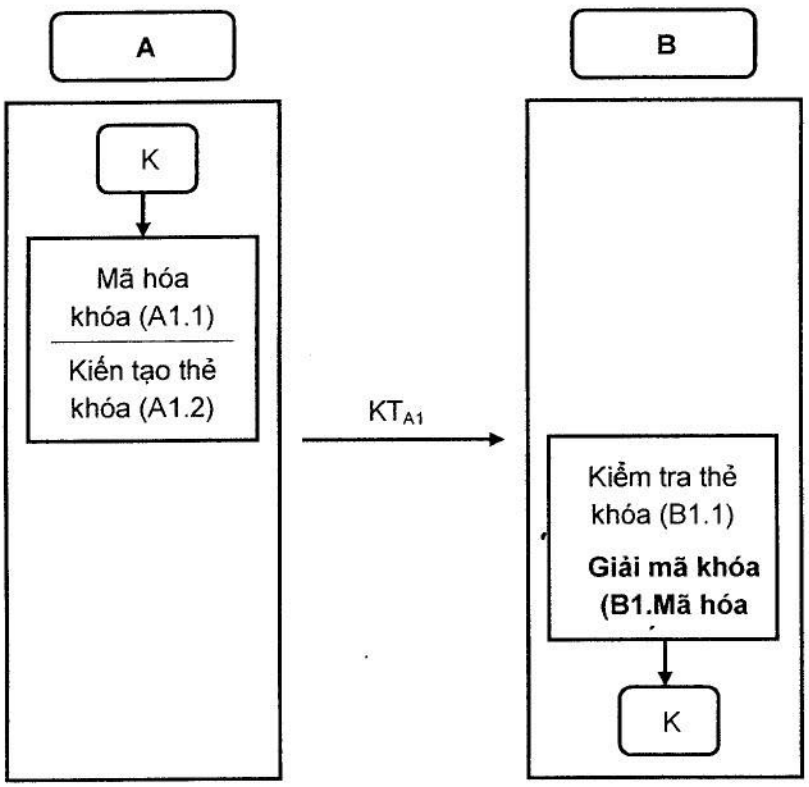
Cơ chế vận chuyển khóa này là một mở rộng của cơ chế xác thực thực thể một lần truyền trong ISO/IEC 9798-3. Nó truyền một khóa bí mật được mã hóa và ký từ một thực thể *A* đến một thực thể *B* có cung cấp tính xác thực khóa ẩn từ *A* đối với *B*. Đối với cơ chế này, các yêu cầu sau cần được thỏa mãn:

1. Thực thể *A* có một hệ chữ ký phi đối xứng (S_A, V_A).
2. Thực thể *B* có một hệ mã hoá phi đối xứng (E_B, D_B).

3. Thực thể *A* phải truy cập được đến bản sao có xác thực của phép mã hóa công khai E_B của *B*. Điều kiện này có thể đạt được nhờ sử dụng các cơ chế ở điều 8.

4. Thực thể *B* phải truy cập được vào bản sao có xác thực của phép kiểm tra công khai V_A của *A*. Điều kiện này có thể đạt được nhờ sử dụng các cơ chế ở điều 8.

5. Cần có một giá trị *TVP* tùy ý có thể là một tem thời gian hoặc một số tuần tự. Nếu tem thời gian được sử dụng thì thực thể *A* và thực thể *B* cần duy trì sự đồng bộ về thời gian hoặc sử dụng một tem thời gian cung cấp bởi bên thứ ba tin cậy. Nếu số tuần tự được sử dụng thì *A* và *B* phải cùng duy trì một bộ đếm.



Hình 9 – Cơ chế vận chuyển khóa 2

Mã hóa khóa (A1.1): *A* có một khóa *K* và muốn chuyển giao nó một cách an toàn sang cho *B*. Trước tiên, *A* tạo ra một khối dữ liệu khóa bao gồm định danh riêng biệt của bên gửi *A*, khóa *K* và trường dữ liệu tùy chọn *Text1*. Sau đó *A* mã hóa khối dữ liệu khóa này bằng phép mã hóa công khai E_B của *B* để tạo thành một khối đã mã như sau:

$$BE = E_B(A \,||\, K \,||\, Text1)$$

Kiến thiết thẻ khóa (A1.2): *A* tạo ra khối dữ liệu thẻ bao gồm định danh riêng biệt bên nhận *B*, một tem thời gian hoặc số tuần tự *TVP*, khối mã *BE* và trường dữ liệu tùy chọn *Text 2*. Tiếp đó, *A* ký khối dữ liệu thẻ này bằng phép ký bí mật S_A của mình và gửi thẻ khóa kết quả sang cho *B*:

$$KT_A = S_A\ (B \parallel TVP \parallel BE \parallel Text2) \parallel Text\ 3$$

Kiểm tra thẻ khóa (B1.1): *B* sử dụng phép kiểm tra công khai của bên gửi V_A để kiểm tra thẻ khóa nhận được KT_A. Tiếp đó, *B* kiểm tra định danh bên nhận *B* và giá trị *TVP*.

Giải mã khóa (B1.2): *B* tiến hành giải mã khối *BE* bằng phép giải mã bí mật D_E của mình. Tiếp đó so sánh trường định danh *A* trong khối *BE* với định danh của thực thể đã ký. Nếu tất cả kiểm tra đều thành công thì *B* chấp nhận khóa *K*.

CHÚ THÍCH: Cơ chế vận chuyển khóa này có các tính chất sau:

1. Số lần truyền: 1.

2. Xác thực khóa và xác thực thực thể: Cơ chế này cung cấp tính xác thực thực thể của *A* đối với *B* nếu trường tùy chọn *TVP* được sử dụng. Ngoài ra, cơ chế này còn cung cấp tính xác thực khóa ẩn của *B* đối với *A*.

3. Xác nhận khóa: Có sự xác nhận khóa của *A* đối với *B*. *B* có thể đảm bảo rằng nó chia sẻ chính xác khóa với *A* nhưng *A* thì chỉ có thể đảm bảo rằng *B* thực sự nhận được khóa sau khi có sự phản hồi khẳng định từ *B*.

4. Kiểm soát khóa: *A* có thể lựa chọn khóa.

5. *TVP* (tùy chọn): Cung cấp sự xác thực thực thể của *A* đối với *B* và ngăn ngừa việc dùng lại thẻ khóa. Để ngăn ngừa việc dùng lại khối dữ liệu khóa *BS* thì một giá trị *TVP* thêm vào có thể cũng được bao gồm trong *Text1*.

6. Trường dữ liệu *A*: Định danh riêng biệt của *A* được bao gồm trong khối mã hóa *BE* giúp chống lại việc *A* bị lộ khối khóa mã khi sử dụng bởi thực thể khác. Điều này có thể thực hiện bằng việc so sánh định danh của *A* với chữ ký của *A* trên thẻ.

7. Phù hợp tiêu chuẩn: Cơ chế này phù hợp với tiêu chuẩn ISO/IEC 9798-3, *Entity authentication using a public key algorithm (Xác thực thực thể sử dụng thuật toán khóa công khai)*. KT_{A1} phù hợp vớt thẻ được gửi một lần với cơ chế xác thực mô tả ở điều 5.1.1 của ISO/IEC 9798-3. Thẻ này giúp điều chỉnh việc vận chuyển khóa *K* thông qua sử dụng trường dữ liệu tùy chọn: *Text1* được thay thế bằng *BE* || *Text2*.

8. Chứng chỉ khóa công khai: Trường dữ liệu *Text3* có thể được sử dụng để phân phối chứng chỉ khóa công khai của thực thể *A*. Vì thế, yêu cầu 4 của mục này có thể được giảm nhẹ và chỉ đòi hỏi rằng thực thể *B* phải có khả năng sở hữu một bản sao chứng chỉ của khóa kiểm tra công khai cung cấp bởi CA.

9. Xác thực thực thể lẫn nhau và kiểm soát khóa chung: Nếu hai bước thực thi của cơ chế vận chuyển khóa này được kết hợp với nhau (*A* đến *B* và *B* đến *A)* thì việc xác thực thực thể lẫn nhau và cùng kiểm soát khóa có thể được cung cấp (phụ thuộc vào việc có sử dụng trường *TVP* hay không).

10. Cách sử dụng: Cơ chế vận chuyển khóa này hướng đến sử dụng cho các môi trường mà tính bí mật của các thành phần thông điệp là cần thiết. Chẳng hạn, thông điệp có chứa nhiều phần tử không bí mật cũng như các khóa mã.

11. Ví dụ: Các ví dụ về cơ chế này được mô tả ở điều B.9 và C.7.

7.3 Cơ chế vận chuyển khóa 3

Cơ chế vận chuyển khóa này thực hiện truyền một lần một khóa mã được ký và mã hóa từ thực thể *A* đến thực thể *B* với sự xác thực khóa một bên. Các yêu cầu sau cần được thỏa mãn:

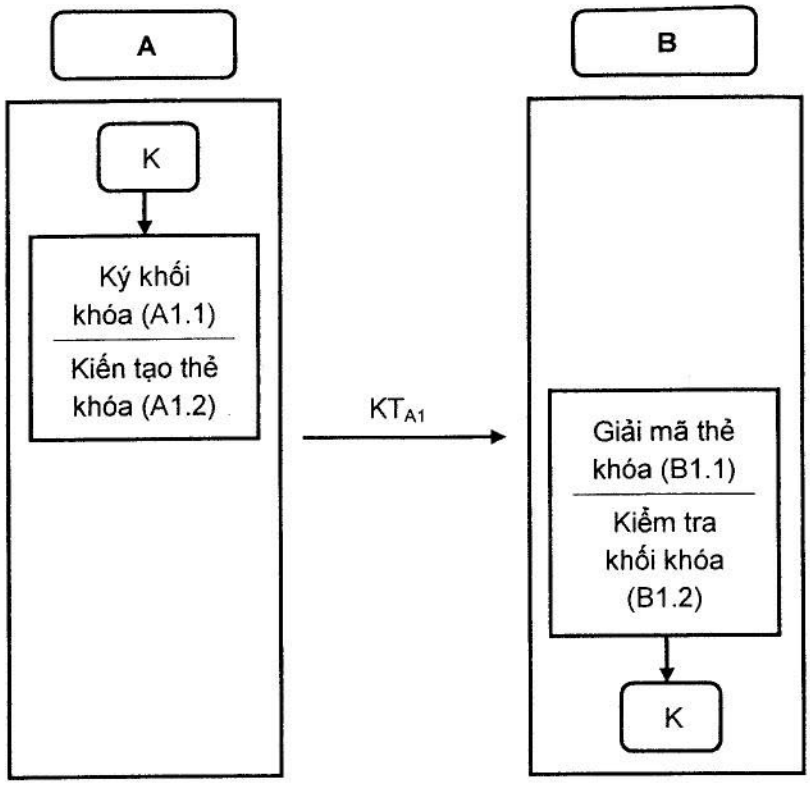
1. Thực thể *A* có một hệ chữ ký phi đối xứng (S_A, V_A).

2. Thực thể *B* có một hệ mật phi đối xứng (E_B, D_B).

3. Thực thể *A* phải truy cập được vào bản sao có xác thực của phép mã hóa công khai E_B của *B*. Điều kiện này có thể đạt được nhờ sử dụng các cơ chế ở điều 8.

4. Thực thể *B* phải truy cập được vào bản sao có xác thực của phép kiểm tra công khai V_A của *A*. Điều kiện này có thể đạt được nhờ sử dụng các cơ chế ở điều 8.

5. Cần có một giá trị *TVP* tùy ý có thể là một tem thời gian hoặc một số tuần tự. Nếu tem thời gian được sử dụng thì thực thể *A* và thực thể *B* cần duy trì sự đồng bộ về thời gian hoặc sử dụng một tem thời gian cung cấp bởi bên thứ ba tin cậy. Nếu số tuần tự được sử dụng thì *A* và *B* phải cùng duy trì một bộ đếm.



Hình 10 – Cơ chế vận chuyển khóa 3

Chữ ký khối khóa (A1.1): *A* có một khóa *K* và muốn truyền bí mật khóa này sang cho *B*. Trước hết *A* tạo ra một khối dữ liệu khóa bao gồm định danh riêng biệt của bên nhận *B*, khóa *K*, một số tuần tự hoặc tem thời gian *TVP* và một vài dữ liệu tùy chọn khác. Tiếp đó *A* ký khối khóa này sử dụng phép ký bí mật S_A của mình để thu được khối đã ký *BS*:

$$BS = S_A(B \,||\, K \,||\, TVP \,||\, Text1)$$

Kiến tạo thẻ khóa (A1.2): *A* tạo ra một khối dữ liệu thẻ bao gồm khối đã ký *BS* và một số giá trị tùy chọn *Text2*. Tiếp đó *A* mã hóa khối dữ liệu thẻ khóa này sử dụng phép mã hóa công khai E_B của bên nhận và gửi kết quả sang cho *B*:

$$KT_{A1} = E_B(BS \,||\, Text2) \,||\, Text3$$

Giải mã thẻ khóa (B1.1): *B* giải mã thẻ khóa KT_{A1} nhận được sử dụng phép giải mã bí mật D_B của mình.

Kiểm tra khối khóa (B1.2): *B* sử dụng phép kiểm tra công khai V_A của bên gửi để kiểm tra tính toàn vẹn và nguồn gốc của *BS*. *B* xác nhận rằng *B* đúng là người nhận thẻ (với sự thẩm tra định danh *B*) và rằng (tùy ý) thẻ đã được gửi theo thời gian xác định (bằng việc thẩm tra *TVP*). Nếu sự xác nhận thành công thì *B* sẽ chấp nhận khóa *K*.

CHÚ THÍCH: Cơ chế vận chuyển khóa này có các tính chất sau:

1. Số lần truyền của giao thức: 1.

2. Xác thực khóa và xác thực thực thể: Cơ chế này cung cấp việc xác thực thực thể của *A* đối với *B* nếu trường tùy chọn *TVP* được sử dụng và cung cấp sự xác thực khóa ẩn của *B* đối với *A*.

3. Xác nhận khóa: Có sự xác nhận khóa của *A* đối với *B*. *B* có thể đảm bảo rằng nó chia sẻ chính xác khóa với *A* nhưng *A* chỉ có thể đảm bảo rằng *B* thực sự nhận được khóa sau khi có sự phản hồi khẳng định từ *B*.

4. Kiểm soát khóa: *A* có thể lựa chọn khóa.

5. *TVP* (tùy chọn): Cung cấp tính xác thực thực thể của *A* đối với *B* và ngăn ngừa việc dùng lại thẻ khóa.

6. Trường dữ liệu *B*: Định danh riêng biệt của *B* được bao gồm trong khối mã hóa *BS* giúp chỉ ra cụ thể bên nhận khóa vì thế chống được việc sử dụng sai khối đã ký *BS* bởi *B*.

7. Các chứng chỉ khóa công khai: Trường dữ liệu *Text3* có thể được sử dụng để phân phối chứng chỉ khóa công khai của thực thể *A*. Vì thế, yêu cầu 4 của mục này có thể được giảm nhẹ rằng chỉ yêu cầu thực thể *B* có được một bản sao chứng chỉ của khóa kiểm tra công khai cung cấp bởi CA.

8. Xác thực thực thể lẫn nhau và kiểm soát khóa chung: Nếu hai bước thực thi của cơ chế vận chuyển khóa này được kết hợp với nhau (*A* đến *B* và *B* đến *A*) thì việc xác thực thực thể lẫn nhau và cùng kiểm soát khóa có thể được cung cấp (phụ thuộc vào việc có sử dụng trường *TVP* hay không).

7.4 Cơ chế vận chuyển khóa 4

Cơ chế vận chuyển khóa này dựa trên cơ chế xác thực hai lần truyền trong ISO/IEC 9798-3 dùng để truyền một khóa bí mật từ thực thể *B* đến thực thể *A*. Các yêu cầu sau cần được thỏa mãn:

1. Thực thể *A* có một hệ mật phi đối xứng (E_A, D_A).

2. Thực thể *B* có một hệ chữ ký phi đối xứng (S_B, V_B).

3. Thực thể *A* phải truy cập được vào bản sao có xác thực của phép kiểm tra công khai V_B của *B*. Điều kiện này có thể đạt được nhờ sử dụng các cơ chế ở mục 8.

4. Thực thể *B* phải truy cập được vào bản sao có xác thực của phép mã hóa công khai E_A của *A*. Điều này có thể đạt được nhờ sử dụng các cơ chế ở mục 8.

Kiến tạo thẻ khóa (A1): *A* tạo ra một thẻ khóa KT_{A1} bao gồm một số ngẫu nhiên r_A và một trường dữ liệu tùy chọn *Text1*:

$$KT_{A1} = r_A \,||\, Text1$$

Và gửi cho *B*.

Mã hóa khối khóa (B1.1): *B* có một khóa *K* muốn gửi an toàn cho *A*. Trước hết *B* tạo ra khối dữ liệu khóa bao gồm định danh riêng biệt của bên gửi *B*, khóa *K* và trường dữ liệu tùy chọn *Text2*. *B* mã hóa khối dữ liệu khóa này bằng phép mã công khai E_A của *A* để được một khối mã:

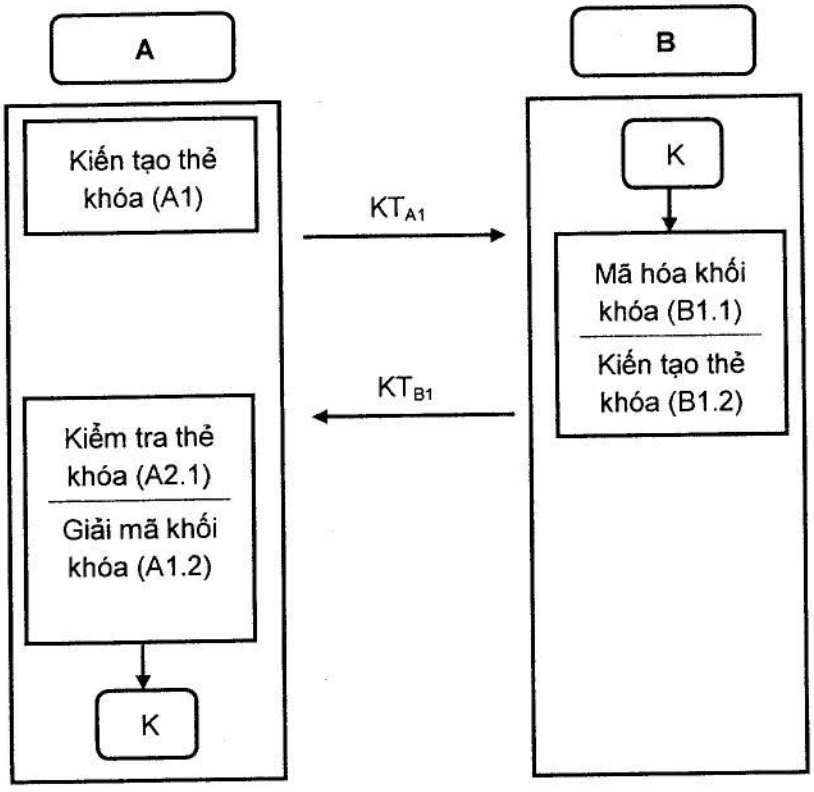
$$BE = E_A\,(B \,||\, K \,||\, Text\ 2)$$

Kiến tạo thẻ khóa (B1.2): *B* tạo ra một khối thẻ khóa bao gồm định danh riêng biệt của bên nhận *A*, số ngẫu nhiên r_A nhận được ở bước 1, số ngẫu nhiên mới r_B (tùy chọn), khối đã mã *BE* và một trường dữ liệu tùy chọn *Text3*. Tiếp đó, *B* tiến hành ký khối dữ liệu thẻ khóa này bằng phép ký bí mật của mình và gửi kết quả cho A:

$$KT_{B1} = S_B\,(A \,||\, r_A \,||\, r_B \,||\, BE \,||\, Text3) \,||\, Text4$$

Kiểm tra thẻ khóa (A2.1): *A* sử dụng phép kiểm tra công khai của bên gửi V_B để kiểm tra chữ ký của thẻ khóa nhận được KT_{B1}. Tiếp đó *A* kiểm tra định danh riêng biệt *A* và kiểm tra giá trị nhận được r_A xem có khớp với số ngẫu nhiên ở bước 1 (A1) hay không.

Giải mã khối khóa (A2.2): *A* tiến hành giải mã khối *BE* bằng phép giải mã bí mật của mình. Tiếp đó, *A* kiểm tra định danh riêng biệt của bên gửi *B*. Nếu tất cả kiểm tra đều thành công thi *A* chấp nhận khóa *K*.



Hình 11 – Cơ chế vận chuyển khóa 4

CHÚ THÍCH: Cơ chế vận chuyển khóa này có các tính chất sau:

1. Số lần truyền: 2.

2. Xác thực khóa và xác thực thực thể: Cơ chế này cung cấp sự xác thực thực thể của *B* đối với *A* và xác thực khóa ẩn của *A* đối với *B*.

3. Xác nhận khóa: Có sự xác nhận khóa của *B* đối với *A*. *A* có thể đảm bảo rằng nó chia sẻ chính xác một khóa *K* với *B* nhưng *B* chỉ có thể đảm bảo rằng *A* nhận được hoàn toàn khóa sau khi nó có được thông điệp an toàn xác nhận từ *A*.

4. Kiểm soát khóa: *B* có thể lựa chọn khóa.

5. Tiêu chuẩn: Phù hợp với ISO/IEC 9798-3, *Entity authentication using a public key algorithm (Xác thực thực thể sử dụng thuật toán khóa công khai)*. Thẻ KT_{A1} và KT_{B1} tương thích với các thẻ được gửi trong cơ chế xác thực hai lần truyền ở điều 5.1.2 của ISO/IEC 9798-3 (chú thích rằng các vai trò của *A* và *B* được biến đổi cho nhau). Thẻ KT_{B1} cung cấp một khóa *K* thông qua việc sử dụng trường dữ liệu tùy chọn *Text2* có thể thay thế bằng *BE* || *Text3*.

6. Phù hợp tiêu chuẩn: Nếu cơ chế vận chuyển khóa này thực thi song song hai hần giữa hai thực thể thì kết quả thu được của cơ chế thỏa thuận khóa lẫn nhau là phù hợp với cơ chế được mô tả trong điều 5.2.3 của ISO/IEC 9798-3, *Two pass parallel authentication (Xác thực song song hai lần truyền)*.

7. Trường dữ liệu r_B: Trường này trình bày để tương thích với ISO/IEC 9798-3. Do đã bao gồm *BE* trong KT_{B1} nên trường r_B không cần thiết phải có và vì thế nó là tùy chọn trong cơ chế này.

8. Xác thực thực thể lẫn nhau và dùng chung khóa: Nếu hai thực thi cơ chế vận chuyển khóa này được kết hợp với nhau (từ *A* đến *B* và từ *B* đến *A*) thì sự xác thực thực thể lẫn nhau và dùng chung khóa được cung cấp.

7.5 Cơ chế vận chuyển khóa 5

Cơ chế vận chuyển khóa này dựa trên cơ chế xác thực ba lần truyền của ISO/IEC 9798-3 dùng để truyền hai khóa bí mật qua ba lần vận chuyển, có cung cấp tính xác thực thực thể lẫn nhau và xác nhận khóa. Một khóa được truyền từ thực thể *A* đến thực thể *B* và một khóa được truyền từ thực thể *B* đến thực thể *A*. Các yêu cầu sau cần phải được thỏa mãn:

1. Mỗi thực thể *X* phải có một hệ chữ ký phi đối xứng (S_X, V_X).

2. Mỗi thực thể *X* phải có một hệ mật phi đối xứng (E_X, D_X).

3. Mỗi thực thể đều có thể truy cập được vào bản sao có xác thực của phép kiểm tra công khai của thực thể kia. Điều kiện này có thể thực hiện được nhờ sử dụng các cơ chế ở điều 8.

4. Mỗi thực thể có thể truy cập được vào bản sao có xác thực của phép mã hóa công khai của thực thể kia. Điều này có thể thực hiện được nhờ sử dụng các cơ chế ở điều 8.

Kiến thiết thẻ khóa (A1): *A* tạo ra một thẻ khóa KT_{A1} bao gồm một số ngẫu nhiên r_A và một trường dữ liệu tùy chọn *Text1* rồi gửi nó cho *B*:

$$KT_{A1} = r_A \,||\, Text1$$

Mã khóa khối khóa (B1.1): *B* có một khóa K_B muốn gửi an toàn cho *A*. Trước hết *B* tạo ra khối dữ liệu khóa bao gồm định danh riêng biệt của bên gửi *B*, khóa K_B và trường dữ liệu tùy chọn *Text2*. *B* mã hóa khối dữ liệu khóa này bằng phép mã công khai E_A của *A* để được một khối mã:

$$BE_1 = E_A\,(B \,||\, K_B \,||\, Text2)$$

Kiến thiết thẻ khóa (B1.2): *B* tạo ra một khối thẻ khóa bao gồm định danh riêng biệt của bên nhận *A*, một số ngẫu nhiên r_A nhận được ở bước 1, một số ngẫu nhiên mới r_B (tùy chọn) do *B* tạo ra, khối đã

mã BE_1 và một trường dữ liệu tùy chọn *Text3*. Tiếp đó, *B* tiến hành ký khối dữ liệu thẻ bằng phép ký bí mật của mình và gửi kết quả cho *A*:

$$KT_{B1} = S_B (r_B \| r_A \| A \| BE_1 \| Text3) \| Text4$$

Kiểm tra thẻ khóa (A2.1): *A* sử dụng phép kiểm tra công khai của bên gửi V_B để kiểm tra chữ ký số của thẻ khóa nhận được KT_{B1}. Tiếp đó *A* kiểm tra định danh riêng biệt *A* và kiểm tra giá trị nhận được r_A xem có khớp với số ngẫu nhiên ở bước 1 (A1) hay không.

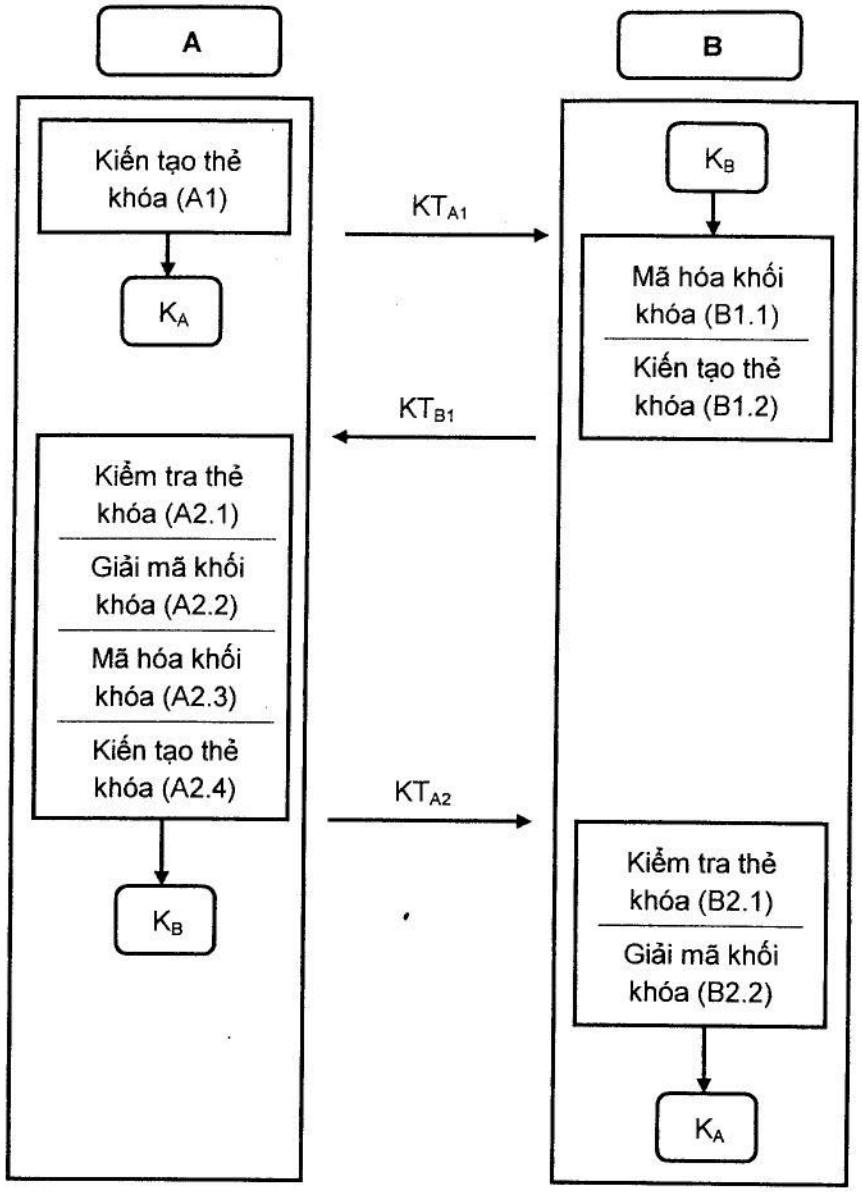
Giải mã khối khóa (A2.2): *A* tiến hành giải mã khối BE_1 bằng phép giải mã bí mật D_A của mình. Tiếp đó, *A* kiểm tra định danh riêng biệt của bên gửi *B*. Nếu tất cả kiểm tra đều thành công thi *A* chấp nhận khóa K_B.

Mã khóa khối khóa (A2.3): *A* có một khóa K_A muốn gửi an toàn cho *B*. Trước hết, *A* tạo ra khối dữ liệu khóa bao gồm định danh riêng biệt của bên gửi *A*, khóa K_A và trường dữ liệu tùy chọn *Text5*. Tiếp đến, *A* mã hóa khối dữ liệu khóa này bằng phép mã công khai E_B của *B* để được một khối mã:

$$BE_2 = E_B (A \| K_A \| Text5)$$

Kiến thiết thẻ khóa (A2.4): *A* tạo ra một khối thẻ khóa bao gồm định danh riêng biệt của bên nhận *B*, một số ngẫu nhiên r_A do *A* tạo ra bước 1 (A1), một số ngẫu nhiên mới r_B do *B* tạo ra ở (B1.2), khối đã mã BE_2 và một trường dữ liệu tùy chọn *Text6*. Tiếp đó, *A* tiến hành ký khối dữ liệu thẻ bằng phép ký bí mật của mình và gửi kết quả cho *B:*

$$KT_{A2} = S_A (r_A \| r_B \| B \| BE_2 \| Text6) \| Text7$$



Hình 12 – Cơ chế vận chuyển khóa 5

Kiểm tra thẻ khóa (B2.1): *B* nhận được KT_{A2} sử dụng phép kiểm tra công khai của bên gửi V_A để kiểm tra chữ ký số của thẻ khóa nhận được KT_{A2}. Tiếp đó *B* kiểm tra định danh riêng biệt *B* của mình và kiểm tra giá trị nhận được r_B xem có khớp với số ngẫu nhiên ở bước (B1.2) hay không. Ngoài ra, *B* cũng kiểm tra giá trị ngẫu nhiên nhận được r_A xem có khớp với số ngẫu nhiên ở bước (A1) hay không.

Giải mã khối khóa (B2.2): *B* tiến hành giải mã khối BE_2 bằng phép giải mã bí mật D_B của mình. Tiếp đó, *B* kiểm tra định danh riêng biệt của bên gửi *A*. Nếu tất cả kiểm tra đều thành công thi *B* chấp nhận khóa K_A.

CHÚ THÍCH: Cơ chế vận chuyển khóa này có các tính chất sau:

1. Số lần truyền: 3.

2. Xác thực khóa và xác thực thực thể: Cơ chế này cung cấp sự xác thực thực thể lẫn nhau, cung cấp xác thực khóa ẩn K_A của *B* đối với *A* và xác thực khóa ẩn K_B của *A* đối với *B*.

3. Xác nhận khóa: Cơ chế này cung cấp tính xác nhận khóa từ bên gửi đến bên nhận đối với cả hai khóa K_A và K_B. Nếu *A* bao gồm giá trị kiểm tra mật mã *Text6* và K_B vào KT_{A2} thì cơ chế này cung cấp sự xác thực khóa lẫn nhau đối với K_B.

4. Kiểm soát khóa: *A* có thể lựa chọn khóa K_A, khi đó *A* là thực thể khởi tạo. Tương tự, *B* có thể lựa chọn thực thể khóa K_B, khi đó *B* lại là thực thể khởi tạo. Việc kiểm soát khóa chung có thể thực hiện bởi mỗi thực thể bằng cách kết hợp hai khóa K_A và K_B của hai bên thành một khuôn dạng khóa bí mật dùng chung duy nhất K_{AB}. Tuy nhiên, hàm kết hợp phải là một chiều, ngoài ra, *A* phải là bên lựa chọn khóa. Cơ chế này có thể xem như là một cơ chế thỏa thuận khóa.

5. Phù hợp tiêu chuẩn: Cơ chế này phù hợp với ISO/IEC 9798-3, *Entity authentication using a public key algorithm (Xác thực thực thể sử dụng thuật toán khóa công khai)*. Các thẻ KT_{A1}, KT_{B1} và KT_{A2} tương thích với các thẻ được gửi trong cơ chế xác thực ba lần truyền ở điều 5.2.2 của ISO/IEC 9798-3. Thẻ KT_{B1} có thể cung cấp một khóa K_B thông qua việc sử dụng trường dữ liệu tùy chọn *Text2* có thể thay thế bằng BE_1 || *Text3*. Thẻ KT_{A2} có thể cung cấp một khóa K_A thông qua việc sử dụng trường dữ liệu tùy chọn *Text4* có thể thay thế bằng BE_2 || *Text6*. Thẻ thứ ba cũng có thể bao gồm một giá trị kiểm tra mật mã *Text6*.

6. Chứng chỉ khóa công khai: Nếu mỗi trường dữ liệu *Text1* và *Text4* (hoặc *Text7* và *Text4*) đều bao gồm chứng chỉ khóa công khai của *A* và *B* thì các yêu cầu 3 và 4 ở điều này có thể làm giảm nhẹ với yêu cầu rằng tất cả thực thể đều phải truy cập được đến bản sao có xác thực của khóa kiểm tra công khai cung cấp bởi CA.

7. Phép biến đổi ký: Nếu một cơ chế chữ ký số có băm văn bản được sử dụng thì số ngẫu nhiều tùy chọn r_A không cần phải gửi kèm theo thẻ khóa KT_{B1}. Tương tự, cả r_A và r_B không cần phải được gửi cùng trong thẻ khóa KT_{A2}. Tuy nhiên, cần phải bao gồm các số ngẫu nhiên để phục vụ cho việc tính toán các chữ ký tương ứng.

7.6 Cơ chế vận chuyển khóa 6

Cơ chế vận chuyển khóa này sử dụng để truyền an toàn hai khóa bí mật bằng ba lần chuyển, một khóa được truyền từ *A* đến *B* và một khóa được truyền từ *B* đến *A*. Ngoài ra, cơ chế này còn cung cấp việc xác thực thực thể lẫn nhau và xác nhận khóa lẫn nhau tương tứng với từng khóa. Cơ chế này dựa trên các yêu cầu sau đây:

1. Mỗi thực thể *X* phải có một hệ mật phi đối xứng (E_X, D_X).

2. Mỗi thực thể có thể truy cập được vào bản sao có xác thực của phép mã hóa công khai của thực thể kia. Điều kiện này có thể thực hiện được nhờ sử dụng các cơ chế ở điều 8.

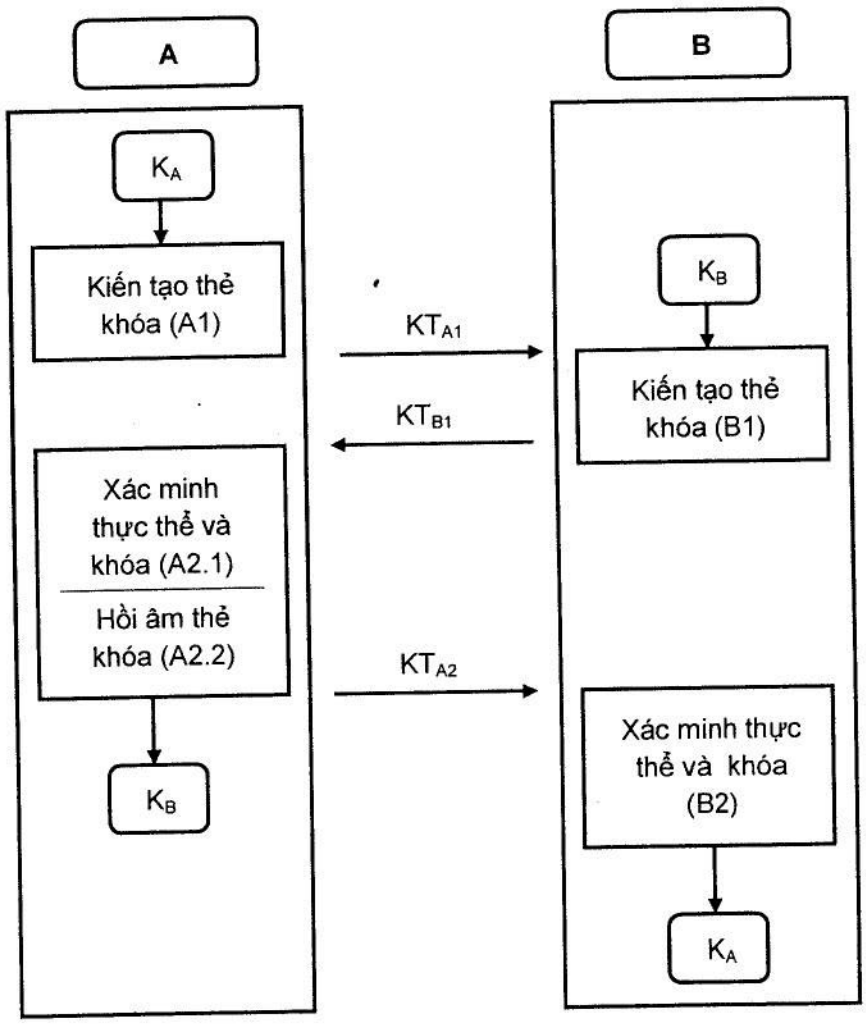
Kiến thiết thẻ khóa (A1): *A* có một khóa K_A muốn gửi an toàn cho *B*. Trước hết, *A* tạo ra một số ngẫu nhiên r_A, Tiếp đến, *A* kiến tạo khối dữ liệu khóa bao gồm định danh riêng biệt của bên gửi *A*, khóa K_A, số ngẫu nhiên r_A và trường dữ liệu tùy chọn *Text1*. *A* mã hóa khối dữ liệu khóa này bằng phép mã công khai E_B của *B* để được một khối mã:

$$BE_1 = E_A\,(A \,||\, K_A \,||\, r_A \,||\, Text1)$$

A lại tạo ra tiếp một thẻ khóa KT_{A1} bao gồm khối dữ liệu đã mã hóa BE_1 và một số trường dữ liệu tùy chọn *Text2*:

$$KT_{A1} = BE_1 \,||\, Text2$$

rồi gửi cho *B*.



Hình 13 – Cơ chế vận chuyển khóa 6

Kiến thiết thẻ khóa (B1): *B* nhận được KT_{A1} sẽ trích rút ra khối khóa đã mã BE_1 rồi tiến hành giải mã bằng phép giải mã bí mật D_B của mình. *B* cũng tiến hành kiểm tra thông tin định danh của bên gửi *A*.

Giả sử *B* có một khóa bí mật K_B muốn gửi an toàn đến cho *A*. Trước hết, *B* lựa chọn một số ngẫu nhiên r_B và kiến tạo ra một khối dữ liệu khóa bao gồm định danh riêng biệt của bên gửi *B*, khóa K_B, số ngẫu nhiê r_B, số ngẫu nhiên r_A nhận được ở bước (A1) và một trường dữ liệu tùy chọn *Text3*. Tiếp đó, *B* tiến hành mã hóa khối dữ liệu khóa bằng phép mã hóa công khai E_A của *A* để tạo ra khối dữ liệu mã:

$$BE_2 = E_A (B \,||\, K_B \,||\, r_A \,||\, r_B \,||\, Text3)$$

Tiếp đó, *B* tạo ra thẻ khóa KT_{B1} bao gồm khối mã BE_2 và một trường dữ liệu tùy chọn *Text4*:

$$KT_{B1} = BE_2 \,||\, Text4$$

rồi gửi cho *A*.

Kiểm tra khóa và thực thể (A2.1): *A* trích rút khối khóa đã mã hóa BE_2 từ thẻ khóa KT_{B1} nhận được và tiến hành giải mã sử dụng phép giải mã bí mật D_A của mình. Tiếp đó, *A* kiểm tra tính hợp lệ của thẻ khóa thông qua việc so sánh số ngẫu nhiên r_A nhận được từ khối BE_2 với số r_A do *A* sinh ra ở bước (A1). Nếu kiểm tra cho kết quả hợp lệ thì *A* đã xác thực được *B* và như thế có nghĩa là khóa K_A đã được gửi an toàn đến *B*.

Hồi âm thẻ khóa (A2.2): *A* trích rút số ngẫu nhiên r_B từ khối đã được giải mã và kiến tạo nên một thẻ khóa KT_{A2} bao gồm số ngẫu nhiên r_B và một trường dữ liệu tùy chọn *Text5*:

$$KT_{A2} = r_B \,||\, Text5$$

rồi gửi sang cho *B*.

Kiểm tra khóa và thực thể (B2): *B* kiểm tra thông tin kiểm tra KT_{A2} để trích rút ra r_B và so sánh với r_B do mình tạo ra. Nếu sự kiểm tra cho kết quả hợp lệ thì *B* đã xác thực được *A*, điều này đồng nghĩa với việc K_B đã được tiếp nhận an toàn bởi *A*.

CHÚ THÍCH: Cơ chế vận chuyển khóa này có các tính chất sau:

1. Số lần truyền: 3.

2. Xác thực khóa và xác thực thực thể: Cơ chế này cung cấp tính xác thực thực thể lẫn nhau, cung cấp xác thực khóa ẩn K_A của *B* đối với *A* và xác thực khóa ẩn K_B của *A* đối với *B*.

3. Xác nhận khóa: Cơ chế này cung cấp sự xác nhận khóa lẫn nhau.

4. Kiểm soát khóa: *A* có thể lựa chọn khóa K_A, khi đó *A* là thực thể khởi tạo. Tương tự, *B* có thể lựa chọn thực thể khóa K_B, khi đó *B* lại là thực thể khởi tạo. Việc kiểm soát khóa chung có thể thực hiện bởi mỗi thực thể bằng cách kết hợp hai khóa K_A và K_B của hai bên thành một khuôn dạng khóa bí mật dùng chung duy nhất K_{AB}. Tuy nhiên, hàm kết hợp phải là một chiều, ngoài ra, *A* phải là bên lựa chọn khóa. Cơ chế này có thể xem như là một cơ chế thỏa thuận khóa.

5. Sử dụng khóa: Cơ chế này sử dụng kỹ thuật phi đối xứng để truyền hai khóa bí mật cho nhau. K_A được truyền từ *A* đến *B* và K_B được truyền từ *B* đến *A*. Các phương pháp sử dụng mật mã riêng biệt sau đây có thể vận dụng từ cơ chế này: *A* sử dụng khóa K_A của nó để mã hóa thông điệp và gửi cho *B* rồi kiểm tra mã xác thực từ *B*. Tiếp đó, *B* sử dụng khóa K_A để giải mã thông điệp và gửi từ *A* và tạo ra mã xác thực gửi trở lại cho *A*. Phương pháp mật mã xuất phát từ *B* cũng thực hiện tương tự. Trong mỗi phương pháp ở đây, cơ sở phi đối xứng của cơ chế vận chuyển khóa có thể được mở rộng để sử dụng các khóa bí mật.

6. Ví dụ: Một ví dụ về cơ chế vận chuyển khóa dạng này là giao thức COMSET (xem bài báo của Brandt ở phần Tài liệu tham khảo).

8 Vận chuyển khóa công khai

Phần này mô tả về các cơ chế quản lý khóa để đưa khóa công khai của các thực thể trở nên khả dụng đối với các thực thể khác theo cách có xác thực. Việc phân phối có xác thực các khóa công khai là một yêu cầu an toàn cơ bản. Điều này có thể thực hiện được theo một số cách khác nhau:

1. Phân phối khóa công khai không cần đến bên thứ ba tin cậy;

2. Phân phối khóa công khai cần đến bên thứ ba tin cậy như thông quan Tổ chức chứng thực (CA).

Khóa công khai của một thực thể *A* là một phần nằm trong thông tin khóa công khai mà *A* muốn công bố. Thông tin khóa công khai này bao gồm ít nhất định danh riêng biệt của *A* và khóa công khai của *A*.

8.1 Phân phối khóa công khai không cần đến bên thứ ba tin cậy

Điều này mô tả về các cơ chế phân phối khóa công khai có xác thực không cần đến bên thứ ba tin cậy.

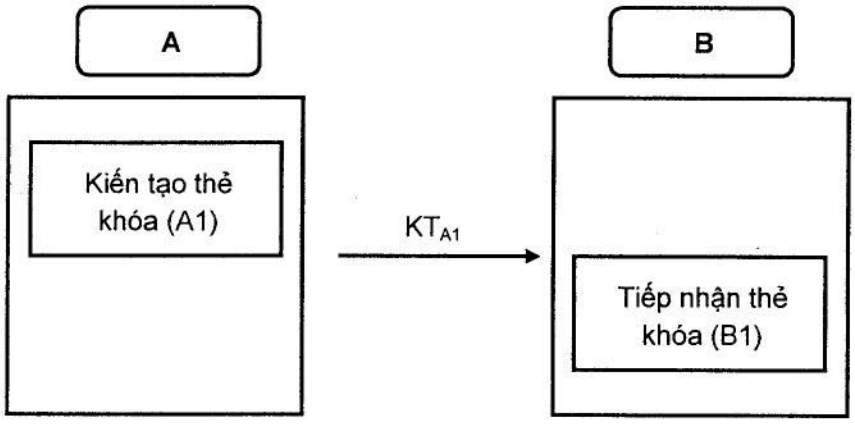
8.1.1 Cơ chế vận chuyển khóa công khai 1

Nếu *A* có thể truy cập vào một kênh được bảo vệ (chẳng hạn kênh có cung cấp tính xác thực nguồn gốc và toàn vẹn dữ liệu) như đường truyền tin thoại, đường truyền thư tín đăng ký trước,...của *B* thì *A*

có thể truyền trực tiếp thông tin khóa công khai cho *B* thông qua các kênh được bảo vệ này. Đây là dạng cơ bản nhất của vận chuyển khóa công khai. Các yêu cầu sau cần phải được thỏa mãn:

1. Thông tin khóa công khai PKI_A của thực thể *A* phải bao gồm ít nhất định danh riêng biệt của *A* và khóa công khai của *A*. Ngoài ra, nó có thể gồm số serial, thời hạn hiệu lực, tem thời gian và một số phần tử thông tin khác.

2. Do thông tin khóa công khai *PKI* không bao gồm bất cứ dạng dữ liệu mật nào nên kênh truyền không cần phải cung cấp tính bí mật.



Hình 14 – Cơ chế vận chuyển khóa công khai 1

Kiến thiết thẻ khóa (A1): *A* tạo ra một thẻ khóa KT_{A1} bao gồm thông tin khóa công khai của *A* và một vài trường dữ liệu tùy chọn *Text* khác. Tiếp đó, *A* gửi thẻ khóa thông qua một kênh truyền có bảo vệ cho *B:*

$$KT_{A1} = PKI_A \,||\, Text$$

Tiếp nhận thẻ khóa (B1): *B* nhận được thẻ khóa từ *A* thông qua kênh truyền được bảo vệ tiến hành bóc tách lấy thông tin khóa công khai PKI_A và lưu trữ khóa công khai của *A* vào một danh sách bao gồm các khóa công khai đang hoạt động (danh sách này được bảo vệ chống lại sự giả mạo hoặc xáo trộn).

CHÚ THÍCH: Cơ chế vận chuyển khóa công khai này có một số tính chất sau:

1. Cơ chế này có thể được sử dụng để truyền các khóa kiểm tra công khai (cho một hệ chữ ký phi đối xứng) hoặc khóa mã công khai (cho một hệ mật phi đối xứng) hoặc khóa thỏa thuận khóa công khai.

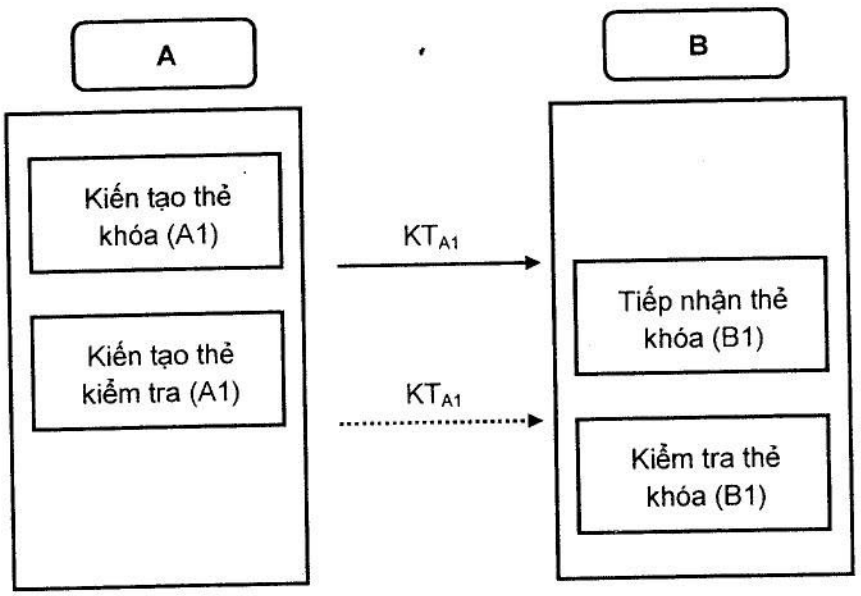
2. Xác thực trong trường hợp này bao gồm cả toàn vẹn dữ liệu và xác thực nguồn gốc dữ liệu (như được đưa ra trong ISO 7498-2:1989).

8.1.2 Cơ chế vận chuyển khóa công khai 2

Cơ chế này truyền thông tin khóa công khai từ một thực thể *A* đến một thực thể *B* bằng kênh truyền không được bảo vệ. Để kiểm tra tính toàn vẹn và nguồn gốc của thông tin khóa công khai nhận được thì một kênh truyền có xác thực thứ hai được sử dụng. Cơ chế này hữu dụng khi thông tin khóa công khai *PKI* được truyền trên kênh băng thông rộng, trong khi việc xác thực thông tin khóa được thực hiện nhờ một kênh truyền băng thông hẹp chẳng hạn như đường tin thoại, đường truyền thư tín đăng ký trước. Một yêu cầu mở rộng là các thực thể có thể chia sẻ chung một hàm băm được định nghĩa trong ISO/IEC 10118-1. Đối với cơ chế này, các yêu cầu sau cần được thỏa mãn:

1. Thông tin khóa công khai PKI_A của thực thể *A* phải bao gồm ít nhất định danh riêng biệt của *A* và thông tin khóa công khai của *A*. Ngoài ra có thể bao gồm số serial, thời gian hiệu lực, tem thời gian và một số phần tử dữ liệu khác.

2. Do thông tin khóa công khai *PKI* không bao gồm bất cứ dạng dữ liệu mật nào nên kênh truyền không cần phải cung cấp tính bí mật.



Hình 15 – Cơ chế vận chuyển khóa công khai 2

Kiến thiết thẻ khóa (A1): *A* tạo ra một thẻ khóa KT_{A1} bao gồm thông tin khóa công khai của *A* và gửi đến cho *B*:

$$KT_{A1} = PKI_A \,||\, Text1$$

Tiếp nhận thẻ khóa (B1): *B* tiếp nhận được thẻ khóa, bóc tách lấy thông tin khóa công khai PKI_A. Hoặc *B* sẽ thực hiện kiểm tra khóa kiểm tra của *A* hoặc sẽ lưu trữ nó ở nơi tránh được giả mạo để cho lần kiểm tra sau hoặc sẽ sử dụng nó.

Kiến tạo thẻ kiểm tra (A2): *A* tính toán giá trị kiểm tra $hash(PKI_A)$ đối với thông tin khóa công khai của nó và gửi giá trị kiểm tra này cùng với các định danh tùy chọn riêng biệt của *A* và *B* rồi gửi đến thực thể *B* sử dụng một kênh truyền có xác thực và độc lập thứ hai (ví dụ kênh truyền điện báo hoặc đường truyền thư đăng ký trước).

$$KT_{A2} = A \,||\, B \,||\, hash(PKI_A) \,||\, Text2$$

Kiểm tra thẻ khóa (B2): Dựa vào thông tin thẻ khóa nhận được KT_{A2}, *B* có thể tùy chọn kiểm tra định danh riêng biệt của *A* và *B*, tính toán ra giá trị kiểm tra trên thông tin khóa công khai của *A* nhận được từ thẻ khóa KT_{A1} và so sánh với giá trị kiểm tra nhận được từ thẻ khóa KT_{A2}. Nếu kết quả kiểm tra thành công thì *B* lấy khóa công khai của *A* đưa lên danh sách các khóa đang hoạt động (danh sách này được bảo vệ chống lại sự giả mạo).

CHÚ THÍCH: Cơ chế vận chuyển khóa công khai này có các tính chất sau:

1. Cơ chế này có thể sử dụng để truyền các khóa kiểm tra công khai (cho một hệ chữ ký phi đối xứng) hoặc khóa mã công khai (cho một hệ mật phi đối xứng) hoặc khóa thỏa thuận khóa công khai.

2. Xác thực trong trường hợp này bao gồm cả toàn vẹn dữ liệu và xác thực nguồn gốc dữ liệu.

3. Nếu khóa công khai được hỗ trợ là một khóa dùng cho hệ chữ ký phi đối xứng không cung cấp tính năng phục hồi thông điệp thì *A* có thể ký thẻ KT_{A1} sử dụng khóa bí mật tương ứng. Trong trường hợp đó, việc kiểm tra chữ ký của *A* ở bước (B1) sử dụng khóa kiểm tra công khai nhận được để xác nhận rằng *A* được biết như là bên có khóa bí mật tương ứng, và rằng chỉ có một thực thể biết khóa bí mật tương ứng tại thời điểm thẻ khóa được tạo ra. Nếu tem thời gian được sử dụng trong *PKI* thì việc kiểm tra để xác nhận rằng *A* hiện đang biết khóa ký bí mật tương ứng.

4. Một chữ ký tay giữa hai bên có thể được sử dụng cho việc kiểm tra thẻ khóa.

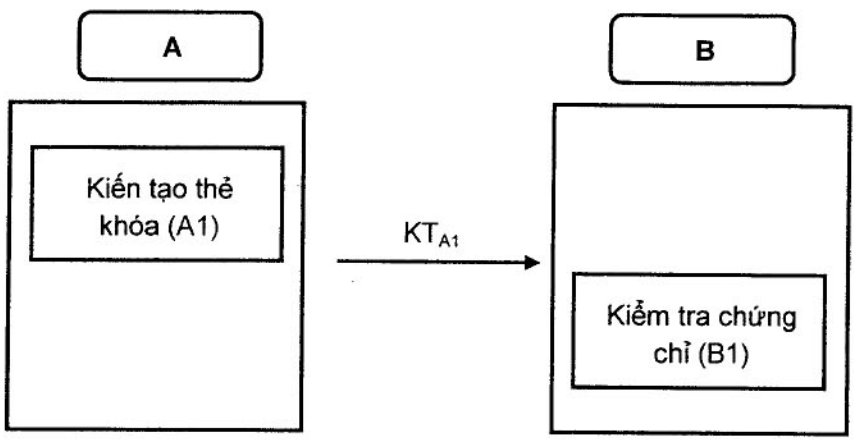
8.2 Phân phối khóa sử dụng bên thứ ba tin cậy

Tính xác thực đối với khóa công khai của các thực thể có thể được đảm bảo bằng cách trao đổi khóa công khai theo khuôn dạng của chứng chỉ khóa công khai. Một chứng chỉ khóa công khai bao gồm thông tin khóa công khai, chữ ký xác nhận lẫn nhau thông qua một bên thứ ba tin cậy là Tổ chức chứng thực (CA). Các tài liệu giới thiệu tại sao CA giúp làm giảm bớt vấn đề về phân phối khóa công

khai có xác thực, việc phân phối khóa có xác thực khóa công khai của CA và chi phí cho trung tâm CA có thể tìm thấy trong ISO/IEC 9594-8 và 11770-1 (Phụ lục A).

8.2.1 Cơ chế vận chuyển khóa công khai 3

Cơ chế này truyền một khóa công khai từ một thực thể *A* đến một thực thể *B* theo phương thức có xác thực. Nó dựa trên giả định rằng chứng chỉ khóa công khai $Cert_A$ hợp lệ của thông tin khóa công khai PKI_A của *A* được ban hành bởi một số Tổ chức chứng thực (CA) và *B* có thể truy cập vào một bản sao có xác thực của phép kiểm tra công khai V_{CA} của Tổ chức chứng thực CA (là bên đã ban hành các chứng chỉ khóa công khai).



Hình 15 – Cơ chế vận chuyển khóa công khai 2

Kiến thiết thẻ khóa (A1): *A* tạo ra một thẻ khóa KT_A bao gồm chứng chỉ khóa công khai của *A* và gửi nó cho *B:*

$$KT_A = Cert_A \,||\, Text$$

Kiểm tra chứng chỉ (B1): Dựa trên thông tin nhận được về chứng chỉ khóa công khai, *B* sử dụng phép kiểm tra công khai V_{CA} của CA để kiểm tra tính xác thực của thông tin khóa công khai và kiểm tra cả tính hợp lệ đối với khóa công khai của *A*.

Nếu *B* muốn đảm bảo rằng chứng chỉ khóa công khai của *A* chưa bị thu hồi ở thời gian hiện hành thì *B* nên tra cứu (tham khảo) một bên thứ ba tin cậy (như một CA) qua một kênh truyền xác thực.

CHÚ THÍCH: Cơ chế vận chuyển khóa công khai này có các tính chất sau:

1. Số lần truyền: 1. Tuy nhiên, có thể xảy ra trường hợp *B* yêu cầu *A* gửi cho *B* một chứng chỉ khóa công khai, trường hợp này không được đề cập ở đây. Chứng chỉ khóa công khai của *A* cũng có thể được phân phối ở một thư mục công khai, trong trường hợp đó cơ chế vận chuyển khóa chỉ được thực hiện giữa *B* và thư mục đó mà thôi.

2. Xác thực thực thể: Cơ chế này không cung cấp tính xác thực thực thể.

3. Xác nhận khóa: Việc nhận một chứng chỉ khóa công khai đã xác nhận rằng khóa công khai đã được chứng nhận bởi một CA.

4. Khóa kiểm tra công khai V_{CA} của CA sẽ được đưa lên sao cho nó luôn khả dụng đối với *B* theo một cách nào đó có cung cấp tính xác thực. Điều này có thể thực hiện được nhờ cơ chế ở điều 8.

Phụ lục A
(tham khảo)

Một số tính chất của các cơ chế thiết lập khóa

Hai bảng sau tổng kết các thuộc tính chính của các cơ chế thiết lập/vận chuyển khóa được đặc tả trong tiêu chuẩn này.

Các ký hiệu được sử dụng trong bảng:

A Cơ chế cung cấp tính chất liên quan đến thực thể *A*.

A,B Cơ chế cung cấp tính chất liên quan đến cả thực thể *A* và thực thể *B*.

Không Cơ chế không cung cấp tính chất này.

opt Cơ chế có thể cung cấp tính chất như một sự tùy chọn nếu có sử dụng các công cụ bổ sung.

(*A*) Cơ chế có thể tùy ý cung cấp tính chất liên quan đến thực thể *A* nếu sử dụng các công cụ tùy chọn.

Số thao tác khóa công khai: Là số lượng phép tính toán khi thực hiện phép biến đổi phi đối xứng. Ví dụ "2,1" có nghĩa là thực thể *A* cần 2 phép tính toán đối với hàm *F* và thực thể *B* cần 1 phép tính toán đối với hàm *F* trong cơ chế thỏa thuận khóa 2.

Các tính chất của các Cơ chế thỏa thuận khóa:

Cơ chế	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Số lần truyền	0	1	1	2	2	2	2
Xác thực khóa ẩn	*A,B*	*B*	*A,B*	Không	*A,B*	*A,B*	*A,B*
Xác nhận khóa	Không	Không	*B*	Không	opt	opt	*A,B*

Xác thực thực thể	Không	Không	(*A*)	Không	Không	*B*	*A,B*
Số thao tác khóa công khai	1,1	2,1	3 (2),2	2,2	2,2	2,2	3,3

Các tính chất của các cơ chế vận chuyển khóa:

Cơ chế	**1**	**2**	**3**	**4**	**5**	**6**
Số lần truyền	1	1	1	2	3	3
Xác thực khóa ẩn	*B*	*B*	*B*	*A*	*A,B*	*A,B*
Xác nhận khóa	Không	*B*	*B*	*A*	(*A*),*B*	*A,B*
Kiểm soát khóa	*A*	*A*	*A*	*B*	*A* đáp *B*	(*A*),*B*
Xác thực thực thể	Không	(A)	(A)	*B*	*A,B*	*A,B*
Số thao tác khóa công khai	1,1	2,2	2,2	4,4	4,4	2,2

Phụ lục B
(tham khảo)

Một số ví dụ về các cơ chế thiết lập khóa

Thông tin cung cấp ở phụ lục này đưa ra các ví dụ về các cơ chế thiết lập khóa đã mô tả trong các phần trước của tiêu chuẩn này.

Trước hết, chúng ta lấy một ví dụ về hàm *F*, cùng với các tập *G* và *H* thỏa mãn 5 tính chất đã liệt kê ở trên, các tham số được chọn một cách thích hợp.

Cho *p* là một số nguyên tố lớn, *G* là tập các phần tử của trường Galois có *p* phần tử ký hiệu là F_p, và tập $H = \{1, \ldots, p-2\}$. Cho *g* là phần tử nguyên thủy của F_p. Thiết lập hàm *F* như sau:

$$F(h,g) = g^h \bmod p$$

Hàm *F* có tích chất giao hoán với đối số là *h* như sau:

$$(g^{h_B})^{h_A} = (g^{h_A})^{h_B} = g^{h_A h_B} \bmod p$$

Số nguyên tố *p* phải đủ lớn để *F(.,g)* có thể được coi là hàm một chiều. Cho thực thể *X* có khóa riêng là h_X thuộc *H*, khóa riêng này chỉ được biết bởi *X*, và một khóa công khai là $p_X = g^{h_X} \bmod p$ được biết bởi tất cả các thực thể.

CHÚ THÍCH: Các chú thích khi lựa chọn tham số:

- Đối với nguyên tố là module logarithm rời rạc: Kích cỡ của số nguyên tố nên được chọn sao cho việc tính logarithm rời rạc trong nhóm cyclic là không thể thực hiện. Một vài điều kiện khác về số nguyên tố có thể được áp đặt để làm cho việc tính logarithm rời rạc là không thể.

- Khuyến cáo để chọn *p* là số nguyên tố mạnh sao cho *p* -1 có thừa số là một số nguyên tố lớn hoặc chọn *g* là một phần tử sinh của một nhóm có bậc nguyên tố lớn *q*.

- Đối với hợp số là module logarithm rời rạc: nên chọn modulus được tạo từ hai số nguyên tố lẻ khác nhau và chúng được giữ bí mật. Kích cỡ của số nguyên tố nên được chọn sao cho việc phân tích modulus là

không thể tính toán được. Một vài điều kiện khác về chọn các số nguyên tố có thể được áp đặt để làm cho việc phân tích modulo là không thể về mặt tính toán.

B.1 Lược đồ thỏa thuận khóa Diffie-Hellman không tương tác

Đây là một ví dụ về Cơ chế thỏa thuận khóa 1.

Kiến thiết khoá (A1): Thực thể *A* sử dụng khóa riêng h_A của mình và khóa công khai p_B của *B* để tính toán ra khóa bí mật dùng chung:

$$K_{AB} = p_B^{\,h_A} \bmod p$$

Kiến thiết khoá (B1): Thực thể *B* sử dụng khóa riêng h_B của mình và khóa công khai p_A của *A* để tính toán ra khóa bí mật dùng chung:

$$K_{AB} = p_A^{\,h_B} \bmod p$$

B.2 Cơ chế dựa trên sự định danh

Đây là một ví dụ về Cơ chế thỏa thuận khóa 1, cơ chế này dựa trên các tiêu chí sau:

- Khóa công khai của một thực thể có thể được nhận từ sự kết hợp giữa định danh và chứng chỉ.
- Tổ chức chứng thực (CA) không tiến hành kiểm tra trực tiếp nhưng chỉ có CA mới có thể phục hồi được một khóa công khai hợp lệ.

Cho (*n*,*y*) là khóa kiểm tra công khai của CA trong cơ chế chữ ký số có phục hồi thông điệp ở Phụ lục A của ISO/IEC 9796. Do *n* được tạo ra từ hai số nguyên tố lớn *p* và *q* và được giữ bí mật bởi CA nên *y* là số nguyên tố cùng nhau với lcm(*p*-1,*q*-1).

Lấy *O* là một số nguyên lớn theo module *n* và $g = O^y \bmod n$.

Lấy I_x là kết quả của phép dư bổ sung (đặc tả ở ISO/IEC 9796) của thông tin công khai trên thực thể *X* có chứa ít nhất một định danh riêng biệt của *X* và có thể có thêm một số serial, thời gian hiệu lực, tem thời gian và một số phần tử dữ liệu khác. Khi đó cặp quản lý khóa của *X* là (h_X,p_X) trong đó h_X là số nguyên nhỏ hơn *n* và:

$$p_X = g^{h_X} (\bmod p).$$

Chứng chỉ được tính bằng CA như sau:

$$Cert_X = s_X O^{h_X} (\mathrm{mod}\, n),$$

Trong đó s_X là một số nguyên sao cho:

$$s_X{}^{y} l_X = 1 (\mathrm{mod}\, n).$$

Kiến thiết khóa (A1): *A* tính toán khóa công khai của *B* như sau:

$$p_B = Cert_B{}^{y}.l_B \bmod n$$

Và tính giá trị khóa bí mật dùng chung như sau:

$$K_{AB} = P_B{}^{h_A} = g^{h_A h_B} \bmod n$$

Kiến thiết khóa (B)1: *B* tính toán khóa công khai của *A* như sau:

$$p_A = Cert_A{}^{y}.l_A \bmod n$$

Và tính giá trị khóa bí mật dùng chung như sau:

$$K_{AB} = P_A{}^{h_B} = g^{h_A h_B} \bmod n$$

CHÚ THÍCH: Cơ chế dựa trên định danh trước một lần truyền hoặc hai lần truyền sử dụng cùng một cách cài đặt mô tả ở tài liệu tham khảo [8], [19] của Phụ lục D (Tài liệu tham khảo).

B.3 Thỏa thuận khóa Elgamal

Đây là ví dụ về Cơ chế thỏa thuận khóa 2.

Cần kiểm tra rằng p là một số nguyên tố mạnh sao cho p - 1 có thừa số là một nguyên tố lớn và các luỹ thừa thì không có dạng 0, +1, -1 mod p.

Kiến thiết thẻ khoá (A1): Thực thể A sinh ngẫu nhiên và bí mật giá trị r thuộc {1, ...,p - 2}, tính g^r mod p và tạo một thẻ khoá KT_{A1} gửi tới B:

$$KT_{A1} = g^r \bmod p$$

Kiến thiết khoá (A2): Tiếp đến, A tính khóa bí mật chia sẻ:

$$KT_{AB} = (p_B)^r \bmod p = g^{h_B r} \bmod p$$

Kiến thiết khoá (B1): Thực thể B tính khóa bí mật dùng chung:

$$KT_{AB} = (g^r)^{h_B} = g^{h_B r} \bmod p$$

B.4 Thỏa thuận khóa Nyberg-Rueppel

Đây là ví dụ về Cơ chế thỏa thuận khóa 3. Hệ chữ ký và hệ thoả thuận khoá được chọn theo cách sao cho hệ chữ ký được xác định bởi các khoá (h_X, p_X).

Cho q là ước nguyên tố lớn của p-1, g là một phần tử thuộc F_p có bậc là q và tập H = {1,...,q-1}. Cặp khóa phi đối xứng của X được sử dụng cho quá trình trao đổi khóa và ký là (h_X,p_X), trong đó h_X là một phần tử thuộc H và $p_X = g^{h_X} (\bmod p)$.

Nhằm ngăn chặn việc sử dụng lặp lại các thẻ khoá cũ, thí dụ này sử dụng một tem thời gian hoặc một số seri *TVP* và một hàm băm mật mã *hash*, nó ánh xạ các chuỗi bit có độ dài bất kỳ vào các số nguyên ngẫu nhiên trong một tập lớn của {1, ... , p-1}, ví dụ, trong H.

Kiến thiết khoá (A1.1): Đầu tiên, thực thể A sinh ngẫu nhiên và bí mật r thuộc H và tính

$$e = g^r \bmod p$$

Tiếp đó, *A* tính khóa bí mật dùng chung là:

$$KT_{AB} = (p_B)^r \bmod p$$

A sử dụng khóa bí mật dùng chung K_{AB} để tính giá trị kiểm tra mật mã trên định danh phân biệt của người gửi và số tuần tự hoặc tem thời gian *TVP*.

$$e' = e.\ hash\ (K_{AB} \| A \| TVP) \bmod p$$

Chữ ký thẻ khoá (A1.2): *A* tính toán chữ ký của thẻ khóa:

$$y' = r - h_A e' \bmod q$$

Cuối cùng, *A* tạo thẻ khóa KT_{A1} và gửi tới *B*:

$$KTA1 = A \| e \| TVP \| y$$

Kiến thiết khoá (B1.1): Thực thể *B* tính khóa bí mật dùng chung sử dụng khóa riêng dùng để thỏa thuận khóa h_B như sau:

$$KT_{AB} = e^{h_B} \bmod p$$

Bằng cách sử dụng khóa bí mật dùng chung K_{AB} vừa tính được, *B* tính giá trị kiểm tra mật mã trên trên định danh phân biệt của người gửi *A* và *TVP* rồi tính:

$$e' = e.\ hash\ (K_{AB} \| A \| TVP) \bmod p$$

Kiểm tra chữ ký (B1.2): *B* kiểm tra tính hợp lệ của *TVP* và sử dụng khóa công khai của p_A để kiểm tra xem đẳng thức sau có đúng hay không:

$$e = g^{y} p_A^{e'} \bmod p$$

B.5 Thỏa thuận khóa Diffie-Hellman

Đây là ví dụ về cơ chế thỏa thuận khóa 4.

Cần kiểm tra rằng *p* là một số nguyên tố mạnh sao cho *p*-1 có thừa số là một nguyên tố lớn và các luỹ thừa không có dạng 0, +1, -1 mod *p*.

Kiến thiết thẻ khoá (A1): Thực thể *A* sinh ngẫu nhiên và bí mật giá trị r_A thuộc {1,...,*p*-2}, tính $g^{r_A} \bmod p$ rồi tạo ra thẻ khoá KT_{A1} và gửi tới *B*:

$$KT_{A1} = g^{r_A} \bmod p$$

Kiến thiết thẻ khoá (B1): Thực thể *B* sinh ngẫu nhiên và bí mật giá trị r_B thuộc {1,...,*p*-2}, tính $g^{r_B} \bmod p$ rồi tạo ra thẻ khoá KT_{B1} gửi tới *A*:

$$KT_{B1} = g^{r_B} \bmod p$$

Kiến thiết khoá (A2): Thực thể *A* tính khóa bí mật dùng chung:

$$K_{AB} = (g^{r_B})^{r_A} \bmod p = g^{r_A r_B} \bmod p$$

Kiến thiết khoá (B2): Thực thể *B* tính khóa bí mật dùng chung:

$$K_{AB} = (g^{r_A})^{r_B} \bmod p = g^{r_A r_B} \bmod p$$

B.6 Lược đồ thỏa thuận khóa Matsumoto-Takashima-Imai A(0)

Đây là ví dụ về Cơ chế thỏa thuận khóa 5.

Cho *p* là một số nguyên tố an toàn và kiểm tra rằng các luỹ thừa không có dạng 0, +1, -1 mod *p*.

Kiến thiết thẻ khoá (A1): Thực thể *A* sinh ngẫu nhiên và bí mật giá trị r_A thuộc {1,...,*p*-2}, tính thẻ khoá KT_{A1} và gửi tới *B*:

$$KT_{A1} = g^{r_A} \bmod p$$

Kiến thiết thẻ khoá (B1): Thực thể *B* sinh ngẫu nhiên và bí mật giá trị r_B thuộc {1,...,*p*-2}, tính thẻ khoá KT_{B1} và gửi tới *A*:

$$KT_{B1} = g^{r_B} \bmod p$$

Kiến thiết khoá (B2): Thực thể *B* tính khóa bí mật dùng chung:

$$K_{AB} = w(KT_{A1}^{h_B}, p_A^{r_B}) = KT_{A1}^{h_B} p_A^{r_B} \bmod p$$

Kiến thiết khoá (A2): Thực thể *A* tính khóa bí mật dùng chung:

$$K_{AB} = w(p_B^{r_A}, KT_{A1}^{h_A}) = KT_{A1}^{h_B} p_A^{r_B} \bmod p$$

B.7 Giao thức Beller-Yacobi

Phần phụ lục này mô tả về giao thức Beller-Yacobi gốc được dùng để minh họa cho Cơ chế thỏa thuận khóa 6.

CHÚ Ý: Lược đồ này không tương thích hoàn toàn với cơ chế thoả thuận khóa 6 bởi vì nó được tối ưu cho các tính huống đặc biệt. Cụ thể, nó sử dụng cơ chế chữ ký ElGamal và sử dụng thêm thuật toán mã hóa đối xứng để chuyển khóa kiểm tra chữ ký của *B* và chứng chỉ số của *B* tới *A* trong một cách tin cậy, bảo đảm tính ẩn danh (anonymity) của *B*.

Cho *enc*: $K \times M \rightarrow C$ là một hàm mã hóa kinh điển, ví dụ như DES, trong đó *K* là không gian khóa, *M* là không gian thông báo, và *C* là không gian mã.

Giả sử S_X ký hiệu phép toán chữ ký ElGamal của thực thể *X*. Quá trình ký được mô tả dưới đây nhấn mạnh sự khác biệt giữa 2 thao tác trực tuyến (on-line) và không trực tuyến (off-line) được yêu cầu trong họ ElGamal của các cơ chế chữ ký.

Chúng ta sử dung P_X và C_X để ký hiệu khóa công khai và chứng chỉ số của thực thể *X*. Phép mã hoá khóa công khai của thực thể *X* (sử dụng khóa P_X) được ký hiệu là E_X (bình phương module trong trường hợp của Rabin).

Tính toán off-line: *B* chọn một giá trị ngẫu nhiên r_B và tính:

$$u = g^{r_B} \bmod p$$

Kiến thiết thẻ khoá (A1): *A* chọn một số ngẫu nhiên r_A và tính KT_{A1} rồi gửi tới *B*:

$$KT_{A1} = (r_A \,||\, A \,||\, C_A)$$

Xử lý thẻ khoá (B1): *B* tạo chữ ký số

$$BS = (u,v) = S_B(r_A \,||\, A)$$

Sau đó chọn một giá trị ngẫu nhiên x_B và tạo KT_{B1} rồi gửi tới A:

$$KT_{B1} = E_A(BS) \,||\, enc\,(u,(B \,||\, P_B \,||\, C_B \,||\, x_B))$$

Kiến thiết khoá (B2): Khóa bí mật dùng chung chính là phần chữ ký của B, u.

Kiến thiết khoá và xác thực thực thể (A2): A giải mã thẻ khoá $E_A(BS)$ để tìm khóa phiên u, sau đó sử dụng hàm mã đối xứng *enc* để giải mã

$$enc\,(u,(B \,||\, P_B \,||\, C_B \,||\, x_B))$$

bằng cách sử dụng khóa phiên u để lấy các thành phần: định danh B, khóa công khai P_B của B, chứng chỉ số C_B của B. A kiểm tra chứng chỉ C_B và thành công thì sau đó nó sử dụng hàm kiểm tra V_B để kiểm tra chữ ký BS của B. Nếu quá trình kiểm tra thành công thì A chấp nhận u là khóa bí mật dùng chung.

B.8 Vận chuyển khóa ElGamal

Phần này là một ví dụ về Cơ chế vận chuyển khóa 1.

Một số nguyên tố thích hợp p và bộ tạo g trên trương Z_P được lựa chọn và đưa ra công khai. Các khóa dùng để thỏa thuận khóa công khai và bí mật của B lần lượt là, h_B và

$$P_B = g^{hB} \bmod p$$

Kiến thiết thẻ khóa (A1): A có một khóa K (trong đó $0 < K < p$) và muốn truyền an toàn sang cho B. Trước hết, A tạo ngẫu nhiên và bí mật một số nguyên r, $1 < r < p$-1 và mã hóa K như sau:

$$BE = K\,(p_B)^r \bmod p$$

Tiếp đó A tạo ra thẻ khóa:

$$KT_{A1} = BE \,||\, g^r \bmod p$$

Và gửi sang cho b.

Tái thiết thẻ khóa (B1): *B* phục hồi khóa *K* sử dụng khóa để thỏa thuận khóa bí mật h_B bằng cách tính:

$$K = BE.\ (g^r)^{hB}\ mod\ p$$

B.9 Vận chuyển khóa ElGamal có chữ ký của bên gửi

Đây là ví dụ về Cơ chế vận chuyển khóa 2.

Một số nguyên tố thích hợp *p* và bộ tạo *g* thuộc Z_P được lựa chọn và công bố công khai. Các khóa dùng để thỏa thuận khóa công khai tương ứng của *B* là h_B và:

$$p_B = g^{hB}\ mod\ p$$

Các phép biến đổi ký công khai và bí mật của *A* tương ứng ký hiệu là S_A và V_A, (S_A, V_A) có thể được thể hiện ở bất cứ hệ chữ ký nào như chữ ký RSA còn việc kiểm tra chữ ký được đưa ra trong ISO/IEC 9796.

Mã hóa khóa (A1.1): *A* có một khóa *K* và muốn gửi nó theo cách an toàn đến *B*. Trước tiên *A* tạo ngẫu nhiên và bí mật một số nguyên r trong khoảng (1,...,*p*-2) sau đó mã hóa khối dữ liệu khóa *A* || *K* như sau:

$$BE = (A\ ||\ K)\ (p_B)^r\ mod\ p$$

Chú thích rằng *K* phải được chọn theo cách sao cho giá trị (*A* || *K*) phải nhỏ hơn số nguyên tố *p*.

Kiến thiết thẻ khóa (A1.2): *A* tạo ra một khối dữ liệu khóa bao gồm định danh riêng biệt của bên nhận, có thể có tem thời gian hoặc một số tuần tự *TVP*, g^r và khối đã mã hóa *BE*. Tiếp đó *A* ký khối dữ liệu khóa bằng phép ký bí mật S_A của mình rồi gửi sang cho *B:*

$$KT_{A1} = S_A\ (B\ ||\ TVP\ ||\ g^r\ ||\ BE)$$

Kiểm tra thẻ khóa (B1.1): *B* sử dụng phép kiểm tra công khai của bên gửi V_A để kiểm tra chữ ký số của thẻ khóa KT_{A1} nhận được. Tiếp đó *B* kiểm tra định danh bên nhận *B* và trường tùy chọn *TVP*.

Giải mã khóa (B1.2): *B* tiến hành giải mã khối *BE* sử dụng khóa để thỏa thuận khóa bí mật h_B của nó bằng cách tính:

$$A \,||\, K = BE\,(g^r)^{-hB} \bmod p$$

Tiếp đó *B* kiểm tra định danh của bên gửi *A*. Nếu tất cả kiểm tra đều thỏa mãn thì *B* chấp nhận khóa *K*.

B.10 Vận chuyển khóa theo RSA

Đây là ví dụ về Cơ chế vận chuyển khóa 1.

Hệ mật phi đối xứng của *B* bao gồm một module RSA $n = pq$, thành phần công khai e và thành phần bí mật d sao cho $ed = 1 \bmod (p-1)(q-1)$. Giả sử rằng có một bản sao tin cậy của các tham số hệ mật (e,n) của *B*.

Kiến thiết thẻ khóa (A1): *A* có một khóa *K* và muốn truyền đến cho *B*. Giả sử *Text1*, *Text2* và giá trị *TVP* tùy ý đều khác không, giả sử dữ liệu được định dạng theo khuôn dạng thích hợp cho việc xử lý bằng RSA (có thể chứa một số giá trị bù). *A* tạo và gửi cho *B* khối dữ liệu:

$$KT_{A1} = E_B\,(A \,||\, K) = (A \,||\, K)^r \bmod n$$

Tái thiết thẻ khóa (B1): *B* nhận được khối khóa và tính toán:

$$(KT_{A1})^d \bmod n = (A \,||\, K)$$

Bên nhận *B* có thể phân tách thông điệp này từ một thông điệp ngẫu nhiên bằng cách kiểm tra một vài điều kiện bù trong nội dung thông điệp $A \,||\, K$.

Giả sử rằng định danh *A* trong thông điệp phục hồi này có một số giá trị bù có thể dùng để kiểm tra hoặc định dạng mong muốn thì *B* sẽ kiểm tra xem định danh phục hồi được *A* có đúng với định dạng mong muốn hay không và chấp nhận thông điệp này chỉ khi các kiểm tra thỏa mãn.

Phụ lục C
(tham khảo)

Ví dụ về các cơ chế thiết lập khóa dựa trên đường cong elliptic

Mục tiêu của Phụ lục này là trình bày về cách thức các cơ chế thiết lập khóa đã mô tả trong tiêu chuẩn này được thực hiện dựa trên các khái niệm về đường cong elliptic. Phần về các giao thức được trình bày dưới đây khác với phần đã nói trong Phụ lục *B*.

Cơ sở toán học của đường cong elliptic:

Một đường cong elliptic *E* là một đường cong bậc ba thông thường trên một trường *K*. Một đường cong elliptic có thể được mô tả theo một tập nghiệm (x,y) (với $x, y \in K$) của phương trình:

$$Y^2 = X^3 + aX + b$$

với một điểm mở rộng *q* là vô cùng.

Các đường cong elliptic có khả năng thực hiện như một phép toán nhị phân: $E \square E \rightarrow E$, ánh xạ mỗi cặp (P_1,P_2) của một điểm trên *E* vào điểm thứ ba $P_1 \bullet P_2$. Với phép toán này thì *E* là một nhóm abelian với phần tử trung hòa *q*.

Cho P là một điểm nào đó trên đường cong *E*, tạo ra nhóm <*P*> có lực lượng hữu hạn *q* với phép toán của nhóm "•". Khi đó, mỗi phần tử thuộc <*P*> là một lũy thừa $P^{[k]}$ nào đó của *P*, trong đó $P^{[k]}$ là tích *k* lần $(P \bullet P \bullet P \bullet \ldots \bullet P)$.

Phép *mũ rời rạc F(.,P)* trên <*P*> được định nghĩa như sau:

$$F(k,P) = P^{[k]} \text{ với } k \in \{1,\ldots,q\text{-}1\}$$

Chú thích đến giá trị tùy ý *h* với $k \in \{1,\ldots,q\text{-}1\}$ trong đẳng thức:

$$(P^{[h]})^{[k]} = P^{[h].[k]} = (P^{[k]})^{[h]}$$

Trong đó nhóm <*P*> được tạo ra bởi *P* là một nhóm abelian.

Mặt khác, cho một điểm tùy ý *Q* nào đó ∈ <*P*> thì số xác định duy nhất x ∈ {1,...,*q*-1} với $Q = P^{[x]}$ được coi như là logarithm rời rạc của *Q* dựa trên *P*.

Tầm quan trọng mật mã của đường cong elliptic bắt nguồn từ việc khó đoán biết để xác định được logarit rời rạc trên đường cong dựa trên trường hữu hạn. Với hiểu biết hiện nay, điều này còn khó hơn việc phân tích các số nguyên hoặc tính logarit rời rạc trên trường GF(p). Điều này tạo nên khả năng thực thi một hệ thống khóa công khai dựa trên đường cong elliptic với số lượng tham số nhỏ hơn nhiều so với các hệ thống khóa công khai trước đây.

Ký hiệu:

Các khái niệm trên dẫn đến cần làm rõ một số ký hiệu sử dụng trong phụ lục này. Sau đây là giải thích một số ký hiệu:

K là một trường hữu hạn có đúng p^n phần tử, trong đó *p* là một số nguyên tố lớn hơn 3, *n* là một số nguyên dương

E là một đường cong elliptic trên *K* và *P* là một điểm trên *E* tạo nên một nhóm <*P*> của phần tử *q*. Giả sử rằng *q* là một số nguyên tố và tập *H* = {1,...,*q*-1}.

Mỗi thực thể *X* có một khóa bí mật h_X thuộc *H* chỉ được biết bởi *X* và một khóa công khai $P_X = G^{[hX]}$ được biết bởi tất cả thực thể khác.

Chú thích rằng các *khóa bí mật* chỉ là các *số nguyên thông thường*, ngược lại các *khóa công khai* là các điểm trên một *đường cong*. Điều này nói lên rằng hệ thống khóa công khai xây dựng dựa trên các logarit rời rạc theo modulo của một số nguyên tố, trong đó cả khóa bí mật và khóa công khai là đối tượng của cùng một kiểu. Có sự khác nhau giữa hai kiểu khóa trong một đường cong, đó là lý do tại sao phải đưa ra một hàm bổ sung ánh xạ các điểm thuộc <*P*> vào các số nguyên thuộc *H*, đây tương tự như một bản dịch chuyển các giao thức ở Phụ lục B sang dạng sử dụng đường cong elliptic.

Như vậy, cho π: <*P*> → *H* là một hàm sao cho việc tổ hợp π và *F(.,P)* cho bởi

$$k \rightarrow P^{[k]} \rightarrow \pi(P^{[k]})$$

là hàm một chiều.

CHÚ THÍCH:

1. Tham số chủ yếu về an toàn của hệ khóa công khai dựa trên đường cong elliptic là kích cỡ của số nguyên tố *q*. Số nguyên *q* phải đủ lớn sao cho *F(.,P)* có thể được xem như là hàm một chiều. Với các thuật toán được biết hiện nay, *F(.,P)* được coi là hàm một chiều nếu *q* có kích cỡ $q > 2^{160}$.

2. Không giống như các hệ thống thuật toán ligarit rời rạc dựa trên trên *GF(p)* (như DSA), có thể chọn các tham số q và p^n xấp xỉ bằng nhau.

3. Có một vài điều kiện đối với p và q (chẳng hạn $p \neq q$) và các tham số đường cong a và b phải được lựa chọn sao cho không có khả năng tính toán được các logarit rời rạc trên đường cong elliptic.

4. Có rất nhiều khả năng tạo ra π, phương pháp đơn giản là chiếu các điểm trên <*P*> lên trục tọa độ và "đọc" phần tử trường này như là một số nguyên theo mod q.

C.1 Thỏa thuận khóa không tương tác kiểu Diffie-Hellman

Đây là một ví dụ về Cơ chế thỏa thuận khóa 1.

Kiến thiết khóa (A1): *A* tính một khóa bí mật dùng chung bằng cách sử dụng khóa dùng để thỏa thuận khóa bí mật h_A của nó và khóa dùng để thỏa thuận khóa công khai P_B của *B* như sau:

$$K_{AB} = (P_B)^{[hA]}.$$

Kiến thiết khóa (B1): *B* tính một khóa dùng chung bằng cách sử dụng khóa dùng để thỏa thuận khóa bí mật h_B của nó và khóa dùng để thỏa thuận khóa công khai P_A của *A* như sau:

$$K_{AB} = (P_A)^{[hB]}.$$

C.2 Thỏa thuận khóa kiểu ElGamal

Đây là ví dụ về Cơ chế thỏa thuận khóa 2.

Kiến thiết thẻ khóa (A1): *A* tạo ngẫu nhiên và bí mật một giá trị r thuộc *H* và tính thẻ khóa như sau:

$$KT_{A1} = (P)^{[r]}.$$

rồi gửi nó cho *B*.

Kiến thiết khóa (A2): *A* tính một khóa bí mật dùng chung như sau:

$$K_{AB} = (P_B)^{[r]} = (P_B)^{[hBr]}$$

Kiến thiết khóa (B2): *B* sử dụng khóa bí mật của mình để tính toán một khóa bí mật dùng chung như sau:

$$K_{AB} = (KT_{A1})^{[hB]} = (P^{[r]})^{[hB]} = (P)^{[r.hB]}$$

C.3 Thỏa thuận khóa theo Nyberg-Rueppel

Đây là ví dụ về Cơ chế thỏa thuận khóa 3.

Giao thức được sử dụng không phải là bản sao chép dạng 1-1 của giao thức ở phần B.3 nhưng dựa trên ý tưởng cơ bản của B.3.

Một hệ chữ ký và một hệ thỏa thuận khóa được chọn sao cho hệ chữ ký được xác định bởi các khóa (h_X, P_X).

Để ngăn ngừa việc dùng lại các thẻ khóa cũ thì ví dụ này sử dụng một tem thời gian hoặc một số tuần tự *TVP* và một hàm băm mật mã *hash*, chẳng hạn như có sự ánh xạ từ chuỗi bít có độ dài tùy ý đến các số nguyên thuộc *H*.

Kiến thiết khóa (A1.1): *A* tạo ngẫu nhiên và bí mật giá trị *r* thuộc *H* và tính:

$$R = P^{[r]}$$

Tiếp đó *A* tính khóa bí mật dùng chung bí mật như sau:

$$K_{AB} = (P_B)^{[r]}$$

A sử dụng khóa bí mật dùng chung này và tính giá trị kiểm tra mật mã tại điểm *R*, định danh riêng biệt của người gửi *A* và số tuần tự hoặc tem thời gian *TVP*:

$$e = hash(R \,||\, K_{AB} \,||\, A \,||\, TVP)$$

Ký thẻ khóa (A1.2): *A* tính chữ ký như sau:

$$KT_A = (R \,||\, A \,||\, TVP \,||\, y)$$

Và gửi nó cho *B*.

Kiến thiết khóa (B1.1): *B* tính khóa bí mật dùng chung sử dụng khóa để thỏa thuận khóa bí mật h_B của mình như sau:

$$K_{AB} = R^{[hB]}$$

B lại sử dụng khóa bí mật dùng chung bí mật này để tính giá trị kiểm tra mật mã đối với định danh riêng biệt của bên gửi *A* và giá trị *TVP* như sau:

$$e = hash(R \,||\, K_{AB} \,||\, A \,||\, TVP)$$

Kiểm tra chữ ký (B1.2): *B* kiểm tra tính hợp lệ của *TVP* và sử dụng khóa công khai của bên gửi P_A để kiểm tra sự bằng nhau:

$$R = P^{[y]}.\ (P_A)^{[e]}.$$

C.4 Thỏa thuận khóa theo kiểu Diffie-Hellman

Phần này là ví dụ về Cơ chế thỏa thuận khóa 4.

Kiến thiết thẻ khoá (A1): Thực thể *A* sinh ngẫu nhiên và bí mật giá trị r_A thuộc *H*, tính thẻ khoá KT_{A1} và gửi tới *B*:

$$KT_{A1} = P^{[rA]}$$

Kiến thiết thẻ khoá (B1): Thực thể *B* sinh ngẫu nhiên và bí mật giá trị r_B thuộc *H*, tính thẻ khoá KT_{B1} gửi tới *A*:

$$KT_{B1} = P^{[rB]}$$

Kiến thiết khoá (A2): Thực thể *A* tính khóa bí mật dùng chung:

$$KT_{AB} = (P^{[rB]})^{[rA]} = P^{[rB]\,[rA]}$$

Kiến thiết khoá (B2): Thực thể *B* tính khóa bí mật dùng chung:

$$KT_{AB} = (P^{[rA]})^{[rB]} = P^{[rA]\,[rB]}$$

C.5 Thỏa thuận khóa theo kiểu Matsumoto-Takashima A(0)

Đây là ví dụ về Cơ chế thỏa thuận khóa 5.

Kiến thiết thẻ khoá (A1): Thực thể *A* sinh ngẫu nhiên và bí mật giá trị r_A thuộc *H*, tính thẻ khoá KT_{A1} và gửi tới *B*:

$$KT_{A1} = P^{[rA]}$$

Kiến thiết thẻ khoá (B1): Thực thể *B* sinh ngẫu nhiên và bí mật giá trị r_B thuộc *H*, tính thẻ khoá KT_{B1} và gửi tới *A*:

$$KT_{B1} = P^{[rB]}$$

Kiến thiết khoá (B2): Thực thể *B* tính khóa bí mật dùng chung:

$$KT_{AB} = w(KT_{A1}^{[hB]}. P_A^{[rB]}).$$

`Trong đó *w* là hàm một chiều.

Kiến thiết khoá (A2): Thực thể *A* tính khóa bí mật dùng chung:

$$KT_{AB} = w(KT_{B1}^{[hA]}. P_B^{[rA]}).$$

C.6 Vận chuyển khóa theo kiểu ElGamal

Phần này là một ví dụ về Cơ chế vận chuyển khóa 1.

Kiến thiết thẻ khóa (A1): *A* có một khóa $K \in H$ và muốn truyền an toàn sang cho *B*. Trước hết, *A* tạo ngẫu nhiên và bí mật một số nguyên $r \in H$ và tính một điểm trên đường cong $P^{[r]}$ rồi mã hóa khóa *K* như sau:

$$BE = (K. \pi ((p_B)^{[r]}))mod\ q$$

Tiếp đó *A* tạo ra thẻ khóa:

$$KT_{A1} = BE \,||\, (p_B)^{[r]})$$

Và gửi sang cho *B*.

Tái thiết thẻ khóa (B1): Để phục hồi khóa K, thực thể B xác định điểm trên đường cong $P^{[r]}$ sử dụng khóa để thỏa thuận khóa bí mật h_B bằng cách tính: $(p_B)^{[r]} = (p_B^{[r]})^{[hB]}$ và bước tiếp đến là tìm ra: $\pi((p_B)^{[r]}))$.

Cuối cùng B thu được khóa K bằng cách tính

$$K = (BE).\pi(((p_B^{[r]})^{[hB]}))^{-1} \bmod q$$

C.6 Vận chuyển khóa theo kiểu ElGamal có chữ ký của bên gửi

Đây là ví dụ về Cơ chế vận chuyển khóa 2.

Các khóa dùng thỏa thuận khóa công khai và bí mật h_B của B tương ứng là:

$$P_B = (P)^{[hB]}.$$

Các phép biến đổi ký công khai và bí mật của A tương ứng ký hiệu là S_A và V_A, (S_A, V_A) có thể được thể hiện ở bất cứ hệ chữ ký nào như chữ ký RSA còn việc kiểm tra chữ ký được đưa ra trong ISO/IEC 9796.

Mã hóa khóa (A1.1): A có một khóa K và muốn gửi nó theo cách an toàn đến B. Trước tiên A tạo ngẫu nhiên và bí mật một số nguyên $r \in H$ và tính hai điểm trên đường cong $P^{[r]}$ và $(P_B)^{[r]}$ rồi mã hóa khối dữ liệu khóa $A \,||\, K$ như sau:

$$BE = (A \,||\, K).\pi((p_B)^{[r]})) \bmod q$$

Chú thích rằng K phải được chọn theo cách sao cho giá trị $(A \,||\, K)$ phải nhỏ hơn số nguyên tố q.

Kiến thiết thẻ khóa (A1.2): A tạo ra một khối dữ liệu khóa bao gồm định danh riêng biệt của bên nhận B, có thể có tem thời gian hoặc một số tuần tự TVP và khối đã mã hóa BE. Tiếp đó A ký khối dữ liệu thẻ bằng phép ký bí mật S_A của mình rồi gửi thẻ khóa thu được sang cho B:

$$KT_{A1} = S_A(B \,||\, TVP \,||\, p^{[r]} \,||\, BE)$$

Kiểm tra thẻ khóa (B1.1): *B* sử dụng phép kiểm tra công khai của bên gửi V_A để kiểm tra chữ ký số của thẻ khóa KT_{A1} nhận được. Tiếp đó *B* kiểm tra định danh bên nhận *B* và trường tùy chọn *TVP*.

Giải mã khóa (B1.2): *B* tiến hành giải mã khối *BE* sử dụng khóa để thỏa thuận khóa bí mật h_B của nó bằng cách tính:

$$A \,||\, K = (BE).\pi\left(\left(\left(p^{[r]}\right)^{[hB]}\right)\right)^{-1} \bmod q$$

Tiếp đó *B* kiểm tra định danh của bên gửi *A*. Nếu tất cả kiểm tra đều thỏa mãn thì *B* chấp nhận khóa *K*.

Tài liệu tham khảo

[1] ANSI X9.30 199x, "Public Key Cryptography Using Irrevarsible Algorithm for the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA)".

[2] ANSI X9.30 199x, "Public Key Cryptography Using Irrevarsible Algorithm for the Financial Services Industry, Part 3: Certificate Management for DSA".

[3] ANSI X9.31 199x, "Public Key Cryptography Using revarsible Algorithm for the Financial Services Industry, Part 4: Management of symmetric algorithm keys using RSA".

[4] Beller M,J., Yacobi Y., "Fully-fledged two-way public authentication and key agreement for low-cost terminals", Electronic Letters Vol 19 no. 11 (27 May '93), pp 999-1001.

[5] RIPE, "Integrity Primitives for Secure Information Systems" – Final Report of RACE Integrity Primitives Evaluation (RIPE-RACE 1040). LNCS 1007, A. Bosselaers, B. Preneel, Eds., Springer-Verlag, 1995.

[6] Diffie W., Hellman M.E., "News Directions in Cryptography", IEEE Trans. on Inform. Theory, vol. IT-22, pp. 644-654, Nov. 1976.

[7] ElGamal, T., "A Public Key Cryptosystem and a Signature Scheme Based on Descrete Logarithms", IEEE Trans. on Inform. Theory, vol. IT-31, pp. 469-472, July 1985.

[8] Girault M., Paillès J.C., "An Identity-based scheme providing zo-ro-knowledge authentication anh authenticated key exchange", Proceedings of ESSORICS 90, pp. 173-184.

[9] ISO 8732:1998, Banking – Key Management (Wholesale).

[10] ISO/IEC 9594-8:1990, (CCITT X.509), "Information Technology – Open Systems Interconnection – The Directory – Authentication framework".

[11] ISO/IEC 9796:1991, "Information technology - Security techniques – Digital signature scheme giving message recovery".

[12] ISO/IEC 10118-2:1994, "Information technology - Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm".

[13] ISO/IEC 10118-3:1998, "Information technology - Security techniques – Hash-functions – Part 3: Dedicated hash functions".

[14] ISO/IEC 10118-4:1998, "Information technology - Security techniques – Hash-functions – Part 4: Mechanisms using modular arithmetic".

[15] ISO 11166-1:1994, "Banking – Key management by means of asymmetric algorithms – Part 1: Principles, Procedures and Formats".

[16] Matsumoto T., Takashima Y., Imai H., "On Seeking Smart Public-Key-Distribution Systems", Trans. of the IECE of Japan, vol. E69 no. 2. Feb. 1986 pp.99-106.

[17] Manezes, A., "Elliptic Curve Public Key Cryptosystem", Kluwer Academic Publishers, 1993.

[18] Nyberg K., Rueppel R.A., "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem", Proceedings of Eurocrypt'94, Springer-Verlag, 1994.

[19] Okamotot E., "Proposal for identity-basded key distribution system", Electronic Letters, Vol. 22, no. 24, 20 Nov. 1986, pp. 1283-1284.

[20] Tanake K., Okamoto E., "Key distribution system fo mail systems using ID-related information directory", Computers & Security, Vol. 10, 1991, pp. 25-23.