TCVN TIÊU CHUẨN QUỐC GIA

TCVN 7817 – 2:2010

ISO/IEC 11770 – 2:2008

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – KỸ THUẬT AN NINH – QUẢN LÝ KHÓA – PHẦN 2: CƠ CHẾ SỬ DỤNG KỸ THUẬT ĐỐI XỨNG

Information technology – Security techniques – Key management
Part 2: Mechanisms using symmetric techniques

HÀ NỘI – 2010

Mục lục **Trang**

Lời nói đầu

TCVN 7817 - 2 : 2010 hoàn toàn tương đương với ISO/IEC 11770 - 2 : 2008.

TCVN 7817 - 2 : 2010 do Tiểu ban Kỹ thuật Tiêu chuẩn quốc gia TCVN/JTC1/SC27 "*Kỹ thuật mật mã*" biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 7817 bao gồm các TCVN sau:

- TCVN 7817 – 1:2007 Công nghệ thông tin – Kỹ thuật mật mã – Quản lý khóa, phần 1: Khung tổng quát.
- TCVN 7817 – 2:2010 Công nghệ thông tin – Kỹ thuật an ninh – Quản lý khóa, phần 2: Cơ chế sử dụng kỹ thuật đối xứng.
- TCVN 7817 – 3:2007 Công nghệ thông tin – Kỹ thuật mật mã – Quản lý khóa, phần 3: Các cơ chế sử dụng kỹ thuật không đối xứng.
- TCVN 7817 – 4:2010 Công nghệ thông tin – Kỹ thuật an ninh – Quản lý khóa, phần 4: Cơ chế dựa trên bí mật yếu.

Công nghệ thông tin – Kỹ thuật an ninh – Quản lý khóa
Phần 2: Cơ chế sử dụng kỹ thuật đối xứng

Information technology – Security techniques – Key management

Part 2: Mechanisms using symmetric techniques

1 Phạm vi áp dụng

Mục đích của quản lý khóa là cung cấp các thủ tục xử lý vật liệu tạo khóa mã hóa được sử dụng trong các thuật toán mã hóa đối xứng và phi đối xứng theo chính sách an ninh bắt buộc. Tiêu chuẩn này qui định các cơ chế thiết lập khóa sử dụng các kỹ thuật mã hóa đối xứng.

Các cơ chế thiết lập khóa sử dụng kỹ thuật mã hóa đối xứng có thể được tạo từ các cơ chế xác thực thực thể trong tiêu chuẩn quốc tế ISO/IEC 9798–2 và ISO/IEC 9798–4 bằng cách chỉ rõ việc sử dụng các trường văn bản sẵn có trong các cơ chế đó. Các cơ chế thiết lập khóa khác tồn tại trong các trường hợp cụ thể xem trong ISO 8732. Bên cạnh việc thiết lập khóa, mục đích của một cơ chế như vậy có thể bao gồm việc xác thực một chiều hoặc xác thực hai chiều của các thực thể đang liên lạc. Các mục đích xa hơn là xác minh tính toàn vẹn của khóa thiết lập hoặc xác nhận khóa.

Tiêu chuẩn này đề cập ba môi trường thiết lập khóa: điểm – điểm, trung tâm phân phối khóa (KDC) và trung tâm chuyển khóa (KTC). Tiêu chuẩn này mô tả về nội dung yêu cầu của các thông điệp mang vật liệu khóa hoặc vật liệu cần thiết để thiết lập các điều kiện chịu ảnh hưởng của các vật liệu khóa được dùng để thiết lập. Tiêu chuẩn này không chỉ ra các thông tin khác được chứa trong thông điệp hoặc chỉ rõ các thông điệp khác như thông điệp lỗi. Các định dạng tường minh của thông điệp không thuộc phạm vi của tiêu chuẩn này.

Tiêu chuẩn này không quy định phương pháp sử dụng để thiết lập các khóa khởi tạo bí mật, tức là tất cả các cơ chế được quy định trong tiêu chuẩn này yêu cầu thực thể chia sẻ khóa bí mật với ít nhất một thực thể khác (ví dụ; một TTP). Hướng dẫn chung về vòng đời của khóa xem trong phần 1 của bộ tiêu chuẩn TCVN 7817. Tiêu chuẩn này không đề cập rõ về các vấn đề quản lý khóa liên miền và không định nghĩa việc thực thi các cơ chế quản lý khóa, các sản phẩm tuân theo tiêu chuẩn này cũng có thể không tương thích.

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 phiên bản được nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng phiên bản mới nhất, gồm cả các sửa đổi.

TCVN 7817–1:2007 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

Định danh phân biệt (distinguishing identifier)

Thông tin để phân biệt rõ một thực thể.

3.2

Xác thực thực thể (entity authentication)

Chứng minh rằng một thực thể là thực thể đã khẳng định.

[ISO/IEC 9798–1]

3.3

Xác thực khóa tường minh từ thực thể A tới thực thể B (explicit key authentication from entity A to entity B)

Sự đảm bảo đối với thực thể B rằng chỉ thực thể A là thực thể khác duy nhất sở hữu khóa đúng.

[TCVN 7817–3]

CHÚ THÍCH Xác thực khóa không tường minh từ A tới B và xác nhận khóa từ A tới B kéo theo xác thực khóa tường minh từ A tới B.

3.4

Xác thực khóa không tường minh từ thực thể A tới thực thể B (implicit key authentication from entity A to entity B)

Sự đảm bảo đối với thực thể B rằng chỉ thực thể A là thực thể khác duy nhất có khả năng sở hữu khóa đúng.

[TCVN 7817–3]

3.5

Xác nhận khóa từ thực thể A tới thực thể B (key confirmation from entity A to entity B)

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

[TCVN 7817–3]

3.6

Kiểm soát khóa (key control)

Khả năng chọn lựa khóa hoặc các tham số được sử dụng khi tính toán khóa.

3.7

Hàm tạo khóa (key generating function)

Hàm lấy một số tham số đầu vào, ít nhất một trong các tham số đó là bí mật và đưa ra khóa phù hợp đối với thuật toán và ứng dụng dự kiến và có đặc tính là không thể tính đầu ra nếu không biết được đầu vào bí mật.

3.8

Thiết lập khóa điểm – điểm (point–to–point key establishment)

Thiết lập khóa trực tiếp giữa các thực thể mà không liên quan đến bên thứ ba.

3.9

Số ngẫu nhiên (random number)

Tham số biến thiên theo thời gian có giá trị không thể đoán trước.

3.10

Độ dư (redundancy)

Thông tin đã biết và có thể kiểm tra.

3.11

Số tuần tự (sequence number)

Tham số biến thiên theo thời gian có giá trị được lấy từ một chuỗi xác định không lặp lại trong một khoảng thời gian nhất định.

3.12

Tham số biến thiên theo thời gian (time variant parameter)

Mục dữ liệu được sử dụng để xác minh rằng một thông điệp không bị phát lại, chẳng hạn như số ngẫu nhiên, số tuần tự hoặc tem thời gian.

4 Ký hiệu và từ viết tắt

$d_K(Z)$	Kết quả giải mã dữ liệu Z với thuật toán mã hóa đối xứng có sử dụng khóa bí mật K
$e_K(Z)$	Kết quả mã hóa dữ liệu Z với thuật toán mã hóa đối xứng có sử dụng khóa bí mật K
f	Hàm tạo khóa
F	Vật liệu tạo khóa
F_X	Vật liệu tạo khóa bắt nguồn từ thực thể X
I_X	Định danh phân biệt của thực thể X
KDC	Trung tâm phân phối khóa
KTC	Trung tâm chuyển khóa
K_{XY}	Khóa bí mật liên kết giữa thực thể X và thực thể Y
MAC	Mã xác thực thông điệp
$MAC_K(Z)$	Kết quả khi áp dụng hàm mã MAC cho dữ liệu Z dùng khóa bí mật K
P	Trung tâm phân phối khóa hoặc Trung tâm chuyển khóa
R	Số ngẫu nhiên
R_X	Số ngẫu nhiên của thực thể X
T/N	Tem thời gian hoặc số tuần tự
TVP	Tham số biến thiên theo thời gian
TVP_X	Tham số biến thiên theo thời gian của thực thể X
T_X / N_X	Tem thời gian hoặc số tuần tự của thực thể X
X | | Y	Kết quả ghép các mục dữ liệu X và Y

Các trường Text1, Text2,... được quy định trong các cơ chế này có thể bao gồm dữ liệu tùy chọn sử dụng trong các ứng dụng nằm ngoài phạm vi của tiêu chuẩn này (có thể bỏ trống các trường này). Mối quan hệ và các nội dung của chúng phụ thuộc vào ứng dụng cụ thể. Một ứng dụng như vậy là xác thực thông điệp (xem ví dụ trong Phụ lục C).

Tương tự như vậy, các trường văn bản rõ tùy chọn có thể được chứa như một tiền tố hoặc phần gắn thêm cho mọi phần của thông điệp. Chúng không bao hàm các vấn đề an ninh và không bao gồm các cơ chế tường minh được quy định trong tiêu chuẩn TCVN 7817.

Các mục dữ liệu tùy chọn trong các cơ chế này được thể hiện trong dấu ngoặc vuông [ ].

5 Các yêu cầu

Các cơ chế thiết lập khóa được quy định trong tiêu chuẩn này sử dụng các kỹ thuật mã hóa đối xứng, cụ thể hơn là thuật toán mã hóa đối xứng, MAC và/hoặc các hàm tạo khóa. Các thuật toán mã hóa và thời gian tồn tại của khóa phải được chọn sao cho không thể tính toán được khóa trong suốt quá trình tồn tại của nó. Nếu các yêu cầu sau không được đáp ứng, thì quá trình thiết lập khóa có thể không thành công.

a) Đối với các cơ chế sử dụng thuật toán mã hóa đối xứng yêu cầu hoặc giả thiết 1 hoặc giả thiết 2:

   1) Thuật toán mã hóa có phương thức hoạt động và độ dư trong bản rõ phải cung cấp cho bên nhận các phương tiện để phát hiện dữ liệu giả mạo hoặc bị sửa đổi.

   2) Tính toàn vẹn của dữ liệu đã mã hóa được đảm bảo bởi MAC.

Các lựa chọn cho thuật toán mã hóa và toàn vẹn tuân theo:

   i) Giả thiết 1) bên trên có thể được bảo đảm nếu sử dụng kỹ thuật mật mã hóa xác thực, khuyến khích sử dụng một trong các kỹ thuật hợp chuẩn trong ISO/IEC 19772.

   ii) Nên chọn thuật toán mã hóa đối xứng trong ISO/IEC 18033–3 và ISO/IEC 18033–4.

   iii) Nếu sử dụng thuật toán mã hóa dạng khối thì các chế độ hoạt động nên theo ISO/IEC 10116.

   iv) Nếu sử dụng MAC, nên chọn các kỹ thuật trong ISO/IEC 9797.

   CHÚ THÍCH 1 Khi liên quan đến KDC hoặc KTC, các giả thiết 1) và 2) không phải luôn luôn tương đương với khả năng phát hiện một cách rõ ràng cuộc tấn công liên kết đang được thực hiện. Xem thêm Phụ lục C.

b) Trong mỗi trao đổi được quy định trong các cơ chế ở Điều 6, 7 và 8 thì bên nhận thông điệp phải biết định danh đã công bố của bên khởi tạo. Nếu không phải trường hợp này, tức là nếu trong trường hợp sử dụng cơ chế không thiết lập định danh đã công bố, thì cuộc trao đổi được thực hiện bằng cách chứa các định danh trong các trường văn bản rõ bổ sung của một hoặc nhiều thông điệp.

CHÚ THÍCH 2 Các đặc tả của cơ chế trong tiêu chuẩn TCVN 7817 yêu cầu tính đúng đắn của định danh chứa trong thông điệp cần được kiểm tra. Điều này phải thực hiện bằng cách so sánh định danh nhận được với các định danh dự kiến (như quy định trong cơ chế có liên quan). Nếu định danh là một chất vấn từ bên khởi tạo thông điệp, bởi vì yêu cầu b) bên trên nên bên nhận phải biết được giá trị của định danh dự kiến.

c) Vật liệu tạo khóa có thể được thiết lập trên các kênh bảo mật hoặc không bảo mật. Khi sử dụng duy nhất kỹ thuật mã hóa đối xứng, thì ít nhất khóa đầu tiên phải được trao đổi giữa hai thực thể sử dụng một kênh bảo mật để cho phép thông tin liên lạc được an toàn.

d) Các cơ chế thiết lập khóa trong tiêu chuẩn này yêu cầu tham số biến thiên theo thời gian, ví dụ tem thời gian, số tuần tự hoặc số ngẫu nhiên. Trong ngữ cảnh này, việc sử dụng thuật ngữ số ngẫu nhiên cũng bao hàm các số giả ngẫu nhiên không thể đoán trước. Các đặc tính của các tham số này chú ý không được lặp lại, đây là điều rất quan trọng cho các cơ chế. Có thể xem thêm thông tin về tham số biến thiên theo thời gian trong Phụ lục B của ISO/IEC 9798–1. Đối với các phương pháp tạo số ngẫu nhiên xem thêm ISO/IEC 18031.

6 Thiết lập khóa điểm – điểm

Sơ đồ quản lý khóa cơ bản là phương pháp thiết lập khóa điểm – điểm, phương pháp này yêu cầu các thực thể phải chia sẻ khóa sao cho các khóa tiếp theo được thiết lập trực tiếp giữa hai thực thể. Trong điều này, có 6 cơ chế thiết lập khóa điểm – điểm được quy định.

Để thực hiện được các cơ chế quy định trong điều này, cần có các điều kiện sau:

a) Khóa K_{AB} là khóa chung của thực thể A và thực thể B,

b) Có ít nhất một trong A và B có khả năng tạo ra, thu được hoặc đóng góp khóa bí mật K, như đã được mô tả trong từng cơ chế,

c) Các yêu cầu bảo mật có liên quan đến tính bảo mật của K và việc phát hiện các thay đổi hoặc phát lại các khóa và thông điệp.

6.1 Cơ chế thiết lập khóa 1

Trong cơ chế thiết lập khóa 1, khóa K được dẫn xuất từ tham số biến thiên theo thời gian TVP, chẳng hạn từ số ngẫu nhiên R, tem thời gian T hoặc số tuần tự N, sử dụng một hàm tạo khóa. Cơ chế thiết lập khóa 1 thiết lập khóa K nhưng không cung cấp xác thực khóa. Cơ chế này yêu cầu A có khả năng tạo ra TVP.

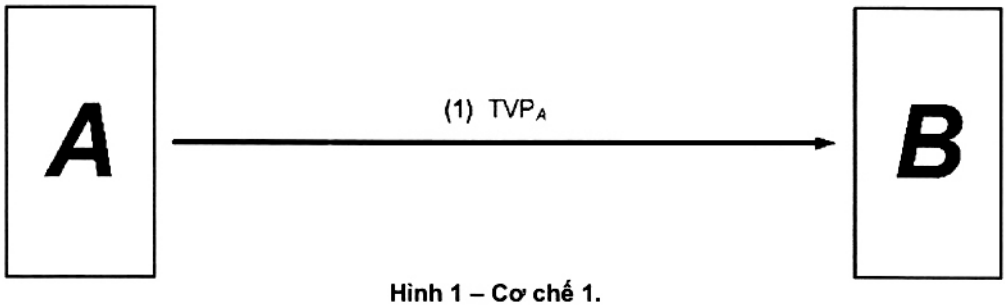
Cơ chế này bao gồm các bước sau (xem Hình 1):

1) A tạo ra tham số biến thiên theo thời gian TVP_A, đó có thể là số ngẫu nhiên R_A, tem thời gian T_A hoặc số tuần tự N_A và chuyển nó cho B.

   i) Cả A và B sau đó tạo khóa K bằng cách sử dụng hàm tạo khóa f mà lấy đầu vào là khóa bí mật dùng chung K_{AB} và tham số biến thiên theo thời gian TVP_A.

$$K = f\,(K_{AB},\ TVP_A).$$

Xem thêm Phụ lục C về ví dụ các hàm tạo khóa.

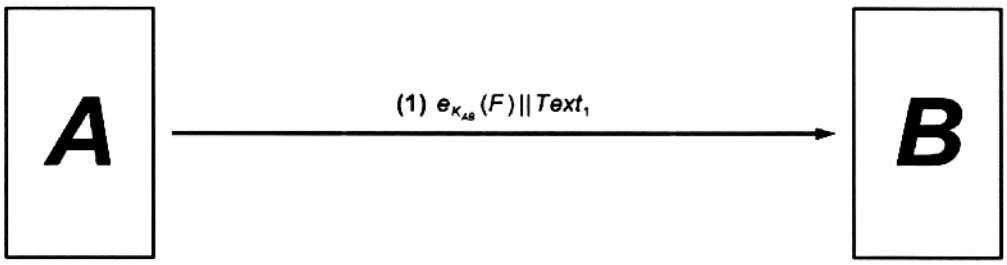


Hình 1 – Cơ chế 1.

CHÚ THÍCH Để có thể đồng thời cung cấp xác thực thực thể, cơ chế thiết lập khóa 1 có thể kết hợp với một cơ chế xác thực được quy định trong ISO/IEC 9798–2 hoặc ISO/IEC 9798–4. Xem ví dụ trong Phụ lục C.

6.2 Cơ chế thiết lập khóa 2

Trong cơ chế thiết lập khóa 2, khóa K được cung cấp bởi thực thể A. Cơ chế này không cung cấp xác thực khóa K được thiết lập bởi cơ chế hoặc không cung cấp xác thực thực thể.



Hình 2 – Cơ chế 2.

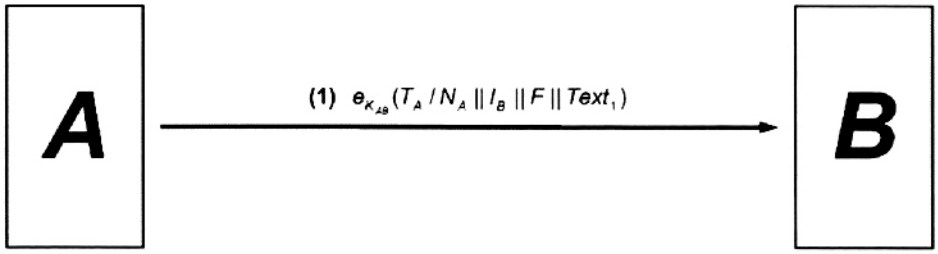
Cơ chế này bao gồm các bước sau (xem Hình 2):

1) A gửi cho B vật liệu tạo khóa F (tạo bởi khóa K và các dữ liệu tùy chọn), mã hóa bằng khóa K_{AB}.

   i. Khi nhận được thông điệp, B giải mã phần mã hóa và do đó có được khóa K.

6.3 Cơ chế thiết lập khóa 3

Cơ chế thiết lập khóa 3 được dẫn xuất từ cơ chế xác thực khóa một chiều với một lần chuyển được quy định trong ISO/IEC 9798–2. Trong cơ chế này, khóa K được cung cấp bởi thực thể A. Cơ chế thiết lập khóa 3 cung cấp xác thực một chiều, tức là cơ chế cho phép thực thể B xác thực thực thể A. Tính duy nhất/ tính thời điểm được kiểm soát bởi các tem thời gian hoặc các số tuần tự. Cơ chế này đòi hỏi cả hai thực thể A và B đều có khả năng duy trì các cơ chế để tạo ra hoặc xác minh tính hợp lệ của tem thời gian T_A hoặc số tuần tự N_A tương ứng.



Hình 3 – Cơ chế 3.

Cơ chế này bao gồm các bước sau (xem Hình 3):

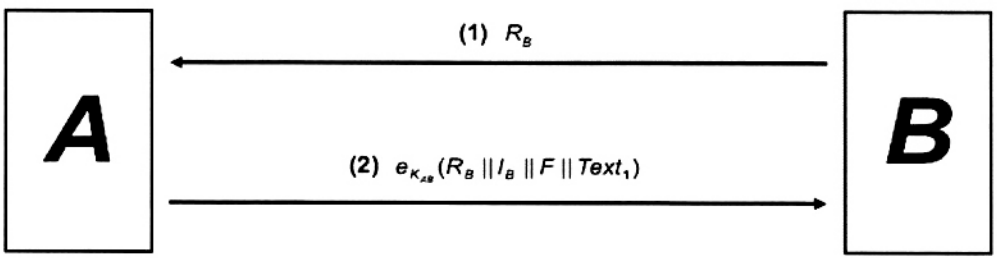
1) A gửi cho B tem thời gian T_A hoặc số tuần tự N_A, định danh phân biệt I_B và vật liệu tạo khóa F (tạo bởi khóa K với dữ liệu tùy chọn). Trong đó định danh phân biệt I_B là tùy chọn. Các trường dữ liệu được mã hóa bằng khóa K_{AB}.

   i) Khi nhận được thông điệp, thực thể B giải mã phần mã hóa, kiểm tra tính đúng đắn của định danh phân biệt (nếu có) và kiểm tra tem thời gian hoặc số tuần tự và cuối cùng lấy ra khóa K.

CHÚ THÍCH Định danh phân biệt I_B bao gồm trong bước 1) để ngăn chặn các kiểu tấn công thứ cấp, tức là thực thể giả mạo B sử dụng lại thông điệp đó gửi đến A (xem thêm trong Phụ lục B). Trong trường hợp mà các kiểu tấn công đó không thể xảy ra thì định danh phân biệt có thể bỏ qua.

6.4 Cơ chế thiết lập khóa 4

Cơ chế thiết lập khóa 4 được dẫn xuất từ cơ chế xác thực khóa một chiều với hai lần chuyển được quy định trong ISO/IEC 9798–2. Trong cơ chế này, khóa K được cung cấp bởi thực thể A. Cơ chế thiết lập khóa 4 cung cấp xác thực một chiều, tức là cơ chế cho phép thực thể B xác thực thực thể A. Tính duy nhất/ tính thời điểm được kiểm soát bởi số ngẫu nhiên R_B. Cơ chế này yêu cầu thực thể B có khả năng tạo ra số ngẫu nhiên.



Hình 4 – Cơ chế 4.

Cơ chế này bao gồm các bước sau (xem Hình 4):

1) B gửi cho A số ngẫu nhiên R_B.

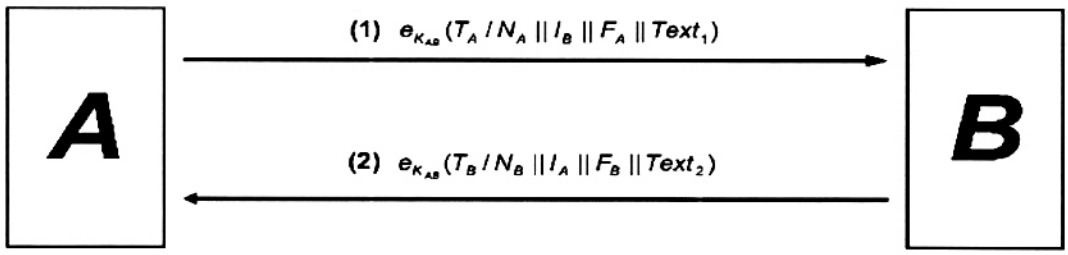
2) A gửi lại cho B số đã nhận được R_B, cùng với định danh phân biệt I_B và vật liệu tạo khóa F (tạo bởi khóa K với dữ liệu tùy chọn). Trong đó định danh phân biệt I_B là tùy chọn. Các trường dữ liệu được mã hóa bằng khóa K_{AB}.

i) Khi nhận được thông điệp 2, thực thể B giải mã phần mã hóa, kiểm tra tính đúng đắn của định danh phân biệt (nếu có) và kiểm tra số ngẫu nhiên R_B (đã gửi cho A ở bước 1) được dùng để tạo thông điệp 2 và cuối cùng lấy ra khóa K.

CHÚ THÍCH Định danh phân biệt I_B bao gồm trong bước 2) để ngăn chặn kiểu tấn công thay thế, tức là thực thể giả mạo B sử dụng lại thông điệp đó gửi đến A (xem thêm Phụ lục B). Trong trường hợp mà kiểu tấn công đó không thể xảy ra thì định danh phân biệt có thể bỏ qua.

6.5 Cơ chế thiết lập khóa 5

Cơ chế thiết lập khóa 5 được dẫn xuất từ cơ chế xác thực khóa hai chiều với hai lần chuyển được quy định trong ISO/IEC 9798 – 2. Cơ chế này cho phép cả hai thực thể A và B cùng tham gia một phần vào thiết lập khóa K. Cơ chế thiết lập khóa 5 cung cấp xác thực hai chiều giữa thực thể A và B. Tính duy nhất/ tính thời điểm được kiểm soát bởi tem thời gian hoặc số tuần tự. Cơ chế này đòi hỏi cả hai thực thể A và B đều có khả năng duy trì các cơ chế để tạo ra hoặc xác minh tính hợp lệ của tem thời gian T hoặc số tuần tự N.



Hình 5 – Cơ chế 5.

Cơ chế này bao gồm các bước sau (xem Hình 5):

1) A gửi cho B tem thời gian T_A hoặc số tuần tự N_A, định danh phân biệt I_B và vật liệu tạo khóa F_A. Trong đó định danh phân biệt I_B là tùy chọn. Các trường dữ liệu được mã hóa bằng khóa K_{AB}.

   i) Khi nhận được thông điệp 1, B giải mã phần mã hóa, kiểm tra tính đúng đắn của định danh phân biệt (nếu có) và kiểm tra tem thời gian hoặc số tuần tự.

2) B gửi cho A tem thời gian T_B hoặc số tuần tự N_B, định danh phân biệt I_A và vật liệu tạo khóa F_B. Trong đó định danh phân biệt I_A là tùy chọn. Các trường dữ liệu được mã hóa bằng khóa K_{AB}.

   i) Khi nhận được thông điệp 2, A giải mã phần mã hóa, kiểm tra tính đúng đắn của định danh phân biệt (nếu có) và kiểm tra tem thời gian hoặc số tuần tự.

   ii) Cả A và B đều tạo ra được khóa K khi sử dụng hàm tạo khóa f, với đầu vào là các trường vật liệu tạo khóa bí mật F_A và F_B.

$$K = f(F_A, F_B).$$

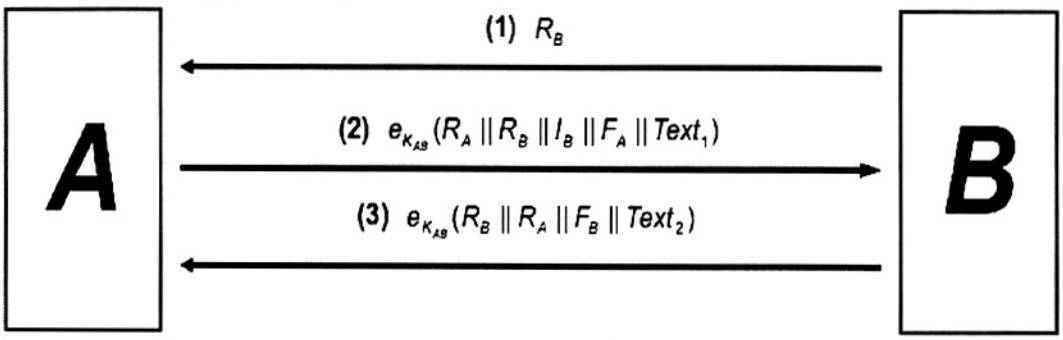
Xem thêm Phụ lục C về một số ví dụ hàm tạo khóa.

Trong cơ chế thiết lập khóa 5, mỗi một trường vật liệu tạo khóa bí mật F_A và F_B có thể là rỗng nhưng không đồng thời cả hai cùng rỗng. Nếu một trong hai trường vật liệu tạo khóa là rỗng, khóa phải được tính toán bằng hàm tạo khóa f như mô tả ở trên nhưng với một trong hai liên kết đầu vào bằng với chuỗi rỗng hoặc chuỗi cố định (tùy thuộc vào tính chất của hàm f).

CHÚ THÍCH Định danh phân biệt I_B bao gồm trong bước 1 để ngăn chặn kiểu tấn công thay thế, tức là thực thể giả mạo B sử dụng lại thông điệp đó gửi đến thực thể A (xem thêm Phụ lục B). Tương tự với trường hợp định danh phân biệt I_A được tạo ra tại bước 2. Nếu trường hợp mà kiểu tấn công này không thể xảy ra thì định danh phân biệt có thể bỏ qua.

6.6 Cơ chế thiết lập khóa 6

Cơ chế thiết lập khóa 6 được dẫn xuất từ cơ chế xác thực khóa hai chiều với ba lần chuyển được xác định trong ISO/IEC 9798 – 2. Trong cơ chế này cho phép cả hai thực thể A và B cùng tham gia một phần trong thiết lập khóa K. Cơ chế thiết lập khóa 6 cung cấp xác thực hai chiều giữa thực thể A và B. Tính duy nhất/ tính thời điểm được kiểm soát bởi số ngẫu nhiên. Cơ chế này đòi hỏi cả hai thực thể A và B đều có khả năng tạo ra số ngẫu nhiên.



Hình 6 – Cơ chế 6

Cơ chế này bao gồm các bước sau (xem Hình 6):

1) B gửi cho A số ngẫu nhiên R_B trong thông điệp 1.

2) A gửi cho B số ngẫu nhiên R_A cùng với số đã nhận R_B, định danh phân biệt I_B và vật liệu tạo khóa F_A trong thông điệp 2. Trong đó định danh phân biệt I_B là tùy chọn. Các trường dữ liệu được mã hóa bằng khóa K_{AB}.

   i) Khi nhận được thông điệp 2, B giải mã phần mã hóa, kiểm tra tính đúng đắn của định danh phân biệt (nếu có) và kiểm tra rằng số ngẫu nhiên R_B đã được gửi cho A ở bước 1 và được dùng để tạo thông điệp 2.

3) B gửi cho A số ngẫu nhiên R_A và R_B và vật liệu tạo khóa F_B trong thông điệp 3. Các trường dữ liệu được mã hóa bằng khóa K_{AB}.

   i) Khi nhận được thông điệp 3, A giải mã phần mã hóa, kiểm tra tính đúng đắn của định danh phân biệt (nếu có) và kiểm tra rằng số ngẫu nhiên R_A và R_B đã được gửi trong thông điệp 1 và 2 tương ứng và được dùng để tạo thông điệp 3 hay không.

ii) Cả A và B đều tạo ra được khóa K khi sử dụng hàm tạo khóa f với đầu vào là các trường vật liệu tạo khóa bí mật F_A và F_B.

$$K = f(F_A, F_B).$$

Xem Phụ lục C có một số ví dụ về hàm tạo khóa.

CHÚ THÍCH 1 Trong cơ chế thiết lập khóa 6, mỗi trường vật liệu tạo khóa bí mật F_A và F_B có thể là rỗng nhưng không đồng thời cả hai cùng rỗng.

CHÚ THÍCH 2 Định danh phân biệt I_B bao gồm trong bước 2 để ngăn chặn kiểu tấn công phản xạ (xem thêm Phụ lục B). Nếu trong trường hợp không thể xảy ra kiểu tấn công này, có thể bỏ qua định danh phân biệt.

CHÚ THÍCH 3 Biến của cơ chế thiết lập khóa 6 được cấu tạo từ hai trường hợp tương đương trong cơ chế thiết lập khóa 4, một biến bắt đầu từ thực thể A và biến còn lại từ thực thể B.

7 Cơ chế sử dụng trung tâm phân phối khóa

Mục đích của trung tâm phân phối khóa (KDC) là đầu tiên tạo ra hoặc thu được và sau đó phân phối khóa cho cặp thực thể mà cùng đã chia sẻ khóa với KDC.

Trong điều này, có 4 cơ chế thiết lập khóa sử dụng KDC được quy định.

- Trong ba cơ chế đầu tiên, một trong hai thực thể yêu cầu khóa K từ KDC để sau đó phân phối cho thực thể còn lại. KDC tạo ra hoặc thu được khóa K và gửi một thông điệp đến thực thể yêu cầu, được bảo vệ bằng khóa đã chia sẻ với thực thể đó. Thông điệp này chứa đựng một thông điệp thứ hai được bảo vệ bởi khóa đã chia sẻ giữa KDC và thực thể thứ hai, sau đó có thể được chuyển tiếp bởi thực thể yêu cầu tới bên nhận cuối cùng.
- Trong cơ chế thứ tư, KDC tạo ra hoặc thu được khóa K và gửi nó trực tiếp đến cả hai thực thể đang giao tiếp. Hai thông điệp được bảo vệ bởi khóa mà KDC đã chia sẻ với các thực thể tương ứng.

Đối với tất cả các cơ chế này, chỉ duy nhất KDC là cần thiết có khả năng tạo ra các khóa hoặc thu được các khóa bằng cách nào đó. Sau khi được phân phối khóa bởi KDC, hai thực thể có thể sử dụng khóa đó hỗ trợ cho cơ chế thiết lập khóa điểm – điểm.

Để thực hiện các cơ chế được quy định trong điều này cần tuân thủ các yêu cầu sau:

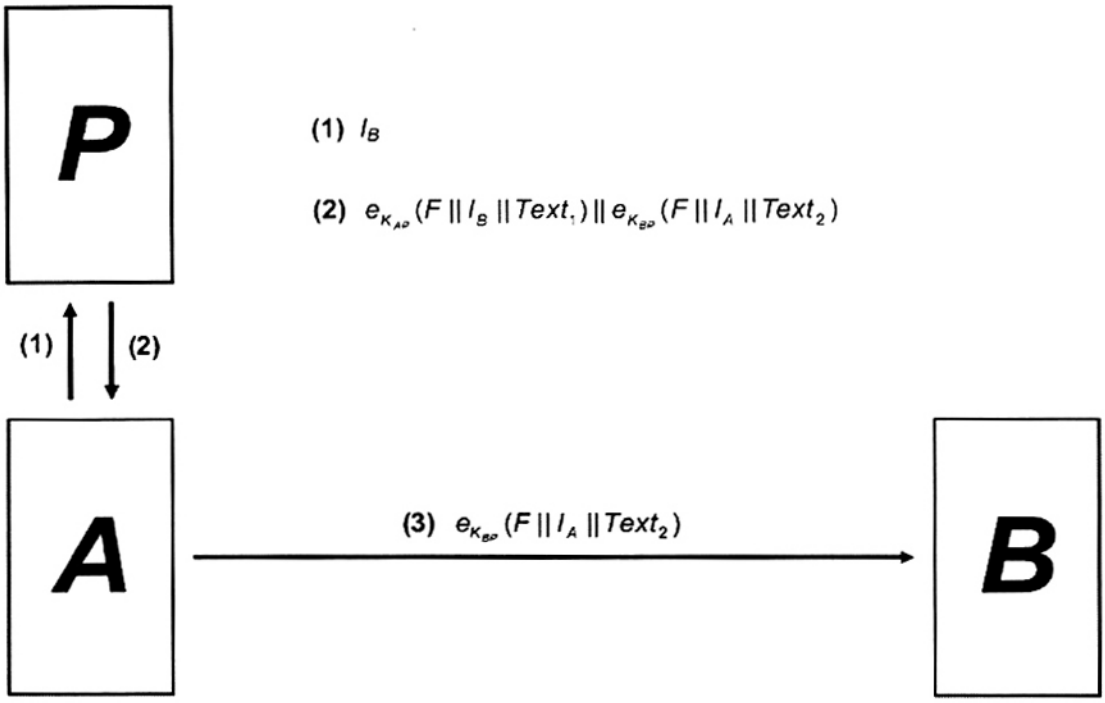
a) Thực thể A và B chia sẻ khóa bí mật K_{AP} và K_{BP} với bên thứ ba đáng tin cậy P (hoạt động như một KDC). KDC phải có khả năng tạo hoặc thu được bằng cách nào đó ra khóa K.

b) KDC phải có một phương pháp giao tiếp với thực thể yêu cầu khóa.

c) Các yêu cầu bảo mật liên quan tới tính bảo mật của khóa K và việc phát hiện sự thay đổi, sự thay thế hoặc phát lại các khóa và thông điệp.

7.1 Cơ chế thiết lập khóa 7

Cơ chế thiết lập khóa 7 không cung cấp xác thực khóa K đã được thiết lập bởi cơ chế.



Hình 7 – Cơ chế 7.

Cơ chế này bao gồm các bước sau (xem Hình 7):

1) A yêu cầu vật liệu tạo khóa từ KDC bằng cách gửi thông điệp 1 tới KDC bao gồm định danh phân biệt I_B của thực thể B.

2) KDC gửi thông điệp 2 cho thực thể A bao gồm vật liệu khóa F (tạo bởi khóa K với dữ liệu tùy chọn). Thông điệp này gồm hai phần:

   - $e_{K_{AP}}$ $(F \| I_B \| Text_1)$;
   - $e_{K_{BP}}$ $(F \| I_A \| Text_2)$.

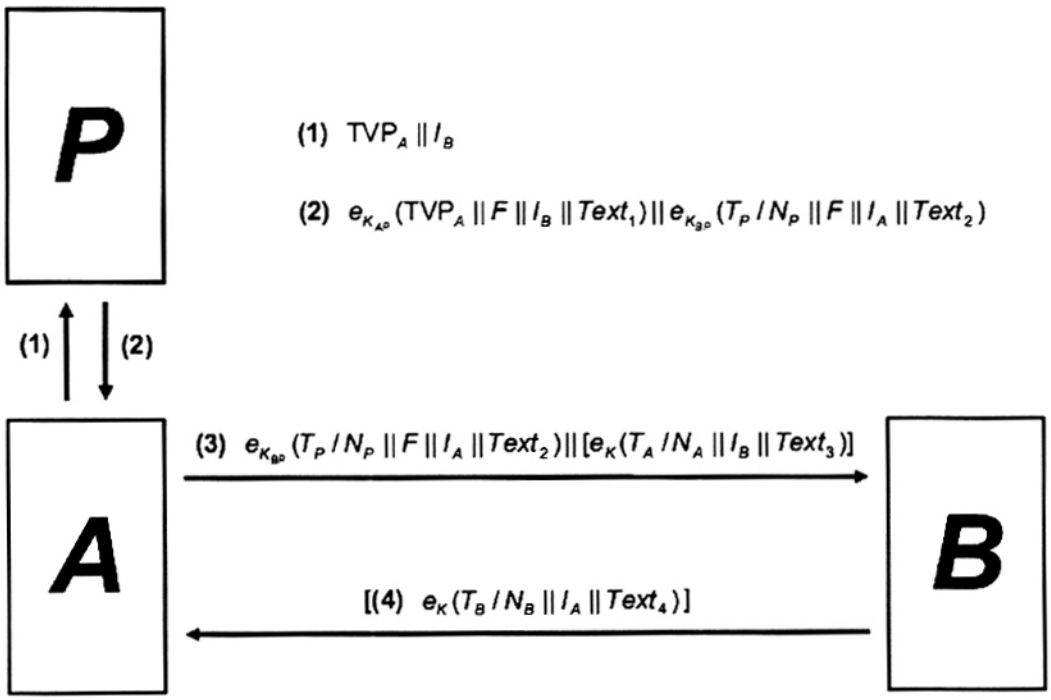
   i) Khi nhận thông điệp 2, thực thể A giải mã phần thứ nhất, kiểm tra tính đúng đắn của định danh phân biệt I_B và thu được khóa K.

3) A chuyển tiếp phần hai của thông điệp 2 cho thực thể B trong thông điệp 3.

   i) Khi nhận thông điệp 3, thực thể B giải mã phần mã hóa, kiểm tra tính đúng đắn của định danh phân biệt I_A và thu được khóa K.

7.2 Cơ chế thiết lập khóa 8

Cơ chế thiết lập khóa 8 được dẫn xuất từ cơ chế xác thực khóa hai chiều với bốn lần chuyển được xác định trong ISO/IEC 9798–2. Cơ chế thiết lập khóa 8 cung cấp xác thực hai chiều giữa thực thể A và B. Tính duy nhất/ tính thời điểm được kiểm soát bởi các tem thời gian hoặc các số tuần tự. Cơ chế này đòi hỏi cả thực thể A và B cùng KDC đều có khả năng duy trì các cơ chế để tạo ra hoặc xác minh tính hợp lệ của tem thời gian T hoặc số tuần tự N.



Hình 8 – Cơ chế 8.

Cơ chế này bao gồm các bước sau (xem Hình 8):

1) A yêu cầu vật liệu tạo khóa từ KDC bằng cách gửi thông điệp 1 tới KDC bao gồm tham số biến thiên theo thời gian TVP_A (có thể là số ngẫu nhiên, tem thời gian hoặc số tuần tự) với định danh phân biệt I_B của thực thể B.

2) KDC gửi thông điệp 2 cho thực thể A chứa đựng vật liệu tạo khóa F (được làm từ khóa K với dữ liệu tùy chọn). Thông điệp này gồm hai phần:

   - $e_{K_{AP}}$ (TVP_A || F || I_B || $Text_1$);
   - $e_{K_{BP}}$ (T_P / N_P || F || I_A || $Text_2$).

   i) Khi nhận được thông điệp 2, thực thể A giải mã phần thứ nhất, kiểm tra tham số biến thiên theo thời gian TVP_A (đã gửi cho KDC tại bước 1) được dùng để tạo nên phần thứ nhất của thông điệp 2, kiểm tra tính đúng đắn của định danh phân biệt I_B và cuối cùng lấy ra khóa K.

3) A chuyển tiếp phần hai của thông điệp 2 cho thực thể B trong thông điệp 3, thông điệp 3 có phần tùy chọn chứa phần thứ hai là trường dữ liệu:

$$e_K(T_A / N_A \| I_B \| Text_3).$$

điều này cho phép thực thể B kiểm tra tính toàn vẹn của khóa K nhận được từ F.

CHÚ THÍCH Tem thời gian T_A hoặc số tuần tự N_A nhận được trong thông điệp 3 là không liên quan đến tham số biến thiên theo thời gian TVP_A nhận được trong thông điệp 1.

i) Khi nhận được thông điệp 3, thực thể B giải mã phần thứ nhất, kiểm tra tính đúng đắn của tem thời gian hoặc số tuần tự, kiểm tra tính đúng đắn của định danh phân biệt I_A và cuối cùng lấy ra được khóa K.

ii) B giải mã phần hai của thông điệp 3 (nếu có) và kiểm tra tính đúng đắn của tem thời gian hoặc số tuần tự và định danh phân biệt I_B.

Bước thứ 4 bên dưới là bước tùy chọn, nó có thể bỏ qua nếu không đòi hỏi xác thực thực thể hoặc xác thực một chiều.

4) B gửi lại $e_K(T_B / N_B \| I_A \| Text_4)$ cho A trong thông điệp 4 qua đó xác nhận việc dùng chung khóa K.

i) Khi nhận được thông điệp 4, A giải mã và kiểm tra tính đúng đắn của tem thời gian hoặc số tuần tự và định danh phân biệt I_A.

CHÚ THÍCH 1 Thuật toán mã hóa e được sử dụng trong quá trình xác nhận khóa tùy chọn (tức là phần 2 của thông điệp 3 và thông điệp 4) có thể khác thuật toán mã hóa (cũng ký hiệu là e) được sử dụng để phân phối khóa.

CHÚ THÍCH 2 Để đạt được mục tiêu xác thực hai chiều và phù hợp với cơ chế xác thực thực thể với 4 lần chuyển được xác định trong ISO/IEC 9798–2 cần bao gồm cả phần thông điệp tùy chọn trong bước 3 và 4.

CHÚ THÍCH 3 Nếu được yêu cầu, việc xác thực của thực thể yêu cầu bởi KDC có thể bao gồm MAC, tính trên TVP_A bằng cách sử dụng khóa bí mật được chia sẻ giữa A và KDC (trong trường bản rõ của thông điệp 1). Nó chỉ làm việc chính xác nếu TVP_A là một mẫu (ví dụ như tem thời gian) đã được xác minh đúng đắn bởi KDC.

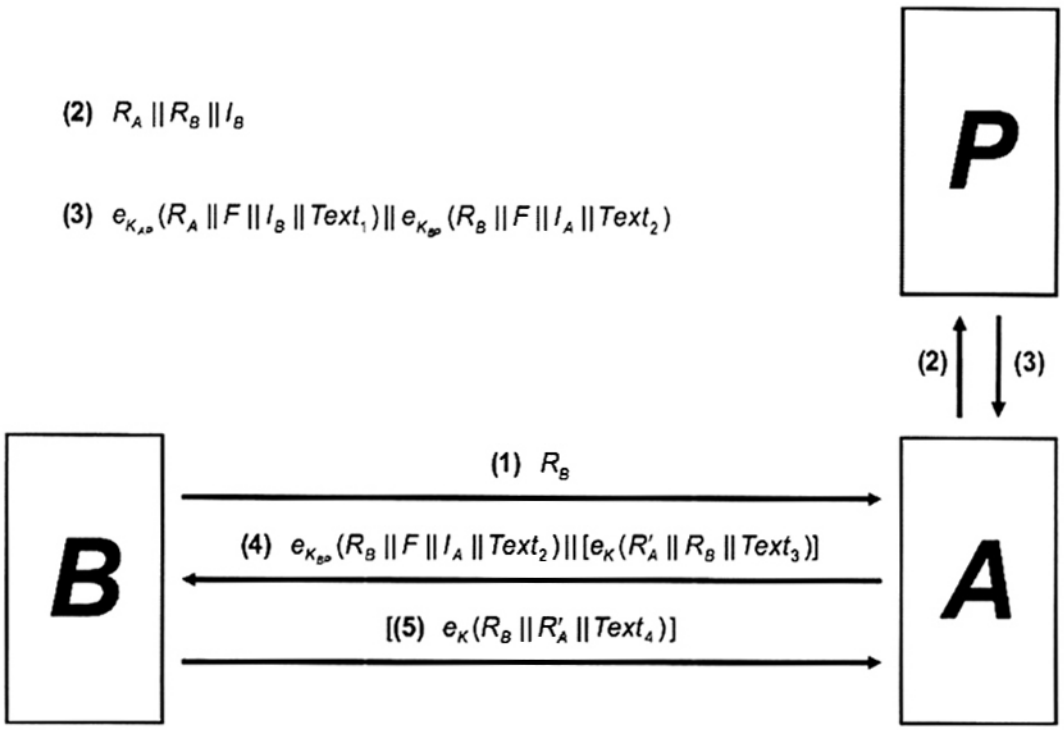
7.3 Cơ chế thiết lập khóa 9

Cơ chế thiết lập khóa 9 được dẫn xuất từ cơ chế xác thực khóa hai chiều với năm lần chuyển được quy định trong ISO/IEC 9798 – 2. Cơ chế thiết lập khóa 9 cung cấp xác thực hai chiều giữa thực thể A và B. Tính duy nhất/ tính thời điểm được kiểm soát bởi số ngẫu nhiên. Cơ chế này đòi hỏi cả thực thể A và B cùng KDC đều có khả năng tạo ra số ngẫu nhiên.

Cơ chế này bao gồm các bước sau (xem Hình 9):

1) B khởi tạo cơ chế bằng cách gửi số ngẫu nhiên R_B cho A trong thông điệp 1.

2) A yêu cầu vật liệu tạo khóa từ KDC bằng cách gửi thông điệp 2 cho KDC bao gồm số ngẫu nhiên R_A, số ngẫu nhiên R_B và định danh phân biệt I_B.



Hình 9 – Cơ chế 9.

3) KDC gửi thông điệp 3 cho thực thể A chứa đựng vật liệu tạo khóa F (được làm từ khóa K với dữ liệu tùy chọn). Thông điệp này chứa hai phần chính:

   – $e_{K_{AP}}$ ($R_A \| F \| I_B \| Text_1$);

   – $e_{K_{BP}}$ ($R_B \| F \| I_A \| Text_2$).

   i) Khi nhận được thông điệp 3, A giải mã phần thứ nhất, kiểm tra số ngẫu nhiên R_A (đã gửi cho KDC tại bước 2 và đã được sử dụng để tạo phần đầu của thông điệp 3), kiểm tra tính đúng đắn của định danh phân biệt I_B và nhận được khóa K.

4) A chuyển tiếp phần hai của thông điệp 3 cho thực thể B trong thông điệp 4 với phần thứ hai tùy chọn là trường dữ liệu:

$$e_K(R'_A \| R_B \| Text_3).$$

đây là kết hợp của số ngẫu nhiên R'_A và R_B và cho phép B kiểm tra được tính toàn vẹn của khóa K thu được từ F.

   i) Khi nhận được thông điệp 4, B giải mã phần thứ nhất, kiểm tra số ngẫu nhiên R_B (đã gửi cho A tại bước 1) có được sử dụng để tạo thông điệp 4 hay không, kiểm tra tính đúng đắn của định danh phân biệt I_A và nhận được khóa K.

   ii) B giải mã phần thứ hai của thông điệp 4 (nếu có) và kiểm tra số ngẫu nhiên R_B (đã gửi cho A tại bước 1) có được sử dụng để tạo phần hai của thông điệp 4 hay không.

Bước thứ 5 tiếp sau là tùy chọn, nó có thể được bỏ qua nếu không đòi hỏi xác thực thực thể hoặc xác thực một chiều. Bước 5 có thể sử dụng nếu phần thứ hai của thông điệp 4 đã được gửi.

5) Thực thể B gửi trả $e_K (R_B || R'_A || Text_4)$ cho A trong thông điệp 5, qua đó xác nhận việc dùng chung khóa K.

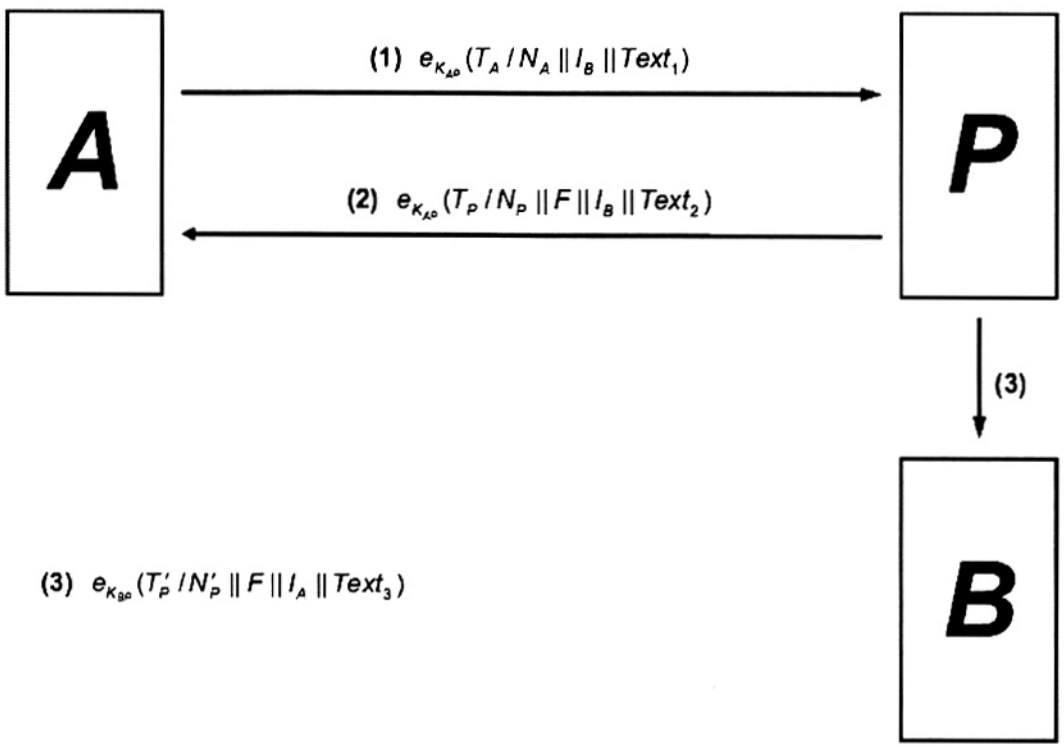
   i) Khi nhận được thông điệp 5, A giải mã và kiểm tra số ngẫu nhiên R'_A (đã gửi cho B trong thông điệp 4 và được dùng để tạo thông điệp 5).

CHÚ THÍCH 1 Thuật toán mã hóa e được sử dụng trong quá trình xác nhận khóa tùy chọn (tức là phần 2 của thông điệp 4 và thông điệp 5) có thể khác thuật toán mã hóa (cũng ký hiệu là e) được sử dụng để phân phối khóa.

CHÚ THÍCH 2 Để đạt được mục tiêu xác thực hai chiều và phù hợp với cơ chế xác thực thực thể với 5 lần chuyển được quy định trong ISO/IEC 9798 – 2 bước 4 và bước 5 cần bao gồm cả thông điệp tùy chọn.

7.4 Cơ chế thiết lập khóa 10

Cơ chế thiết lập khóa 10 cung cấp xác thực hai chiều giữa thực thể A và KDC và xác thực một chiều của KDC cho thực thể B. Tính duy nhất/ tính thời điểm được kiểm soát bởi tem thời gian hoặc số tuần tự. Cơ chế này đòi hỏi cả A và B cùng KDC đều có khả năng duy trì các cơ chế để tạo ra và/hoặc xác minh tính hợp lệ của tem thời gian T hoặc số tuần tự N.



Hình 10 – Cơ chế 10.

Cơ chế này bao gồm các bước sau (xem Hình 10):

1) A yêu cầu vật liệu tạo khóa F từ KDC bằng cách gửi thông điệp 1 bao gồm tem thời gian T_A hoặc số tuần tự N_A và định danh phân biệt I_B của B. Trường dữ liệu được mã hóa bởi khóa K_{AP}.

   i) Khi nhận được thông điệp 1, KDC giải mã và kiểm tra tính đúng đắn của tem thời gian hoặc số tuần tự.

2) KDC gửi thông điệp 2 cho A bao gồm tem thời gian T_P hoặc số tuần tự N_P và định danh phân biệt I_B cùng với vật liệu tạo khóa F (được làm từ khóa K với dữ liệu tùy chọn). Trường dữ liệu được mã hóa bởi khóa K_{AP}.

   i) Khi nhận được thông điệp 2, A giải mã và kiểm tra tính đúng đắn của định danh phân biệt I_B, kiểm tra tính đúng đắn của tem thời gian hoặc số tuần tự và thu được khóa K.

3) KDC gửi thông điệp 3 cho thực thể B bao gồm tem thời gian T'_P hoặc số tuần tự N'_P, định danh phân biệt I_A và vật liệu tạo khóa F. Trường dữ liệu được mã hóa bởi khóa K_{BP} .

   i) Khi nhận được thông điệp 3, B giải mã và kiểm tra tính đúng đắn của tem thời gian hoặc số tuần tự và nhận được khóa K. Định danh phân biệt I_A chỉ ra cho thực thể B rằng khóa được yêu cầu từ thực thể A.

CHÚ THÍCH 1 Thứ tự thực hiện các bước 2 và 3 theo quyết định của hợp đồng.

CHÚ THÍCH 2 Cơ chế này không cung cấp xác thực thực thể giữa A và B. Nếu có yêu cầu xác thực thực thể A và B, thì có thể sử dụng khóa K được thiết lập bởi cơ chế kết hợp với một trong các cơ chế quy định trong ISO/IEC 9798 – 2 hoặc ISO/IEC 9798 – 4.

CHÚ THÍCH 3 Xác thực thực thể cho thực thể yêu cầu do KDC cung cấp.

8 Cơ chế sử dụng trung tâm chuyển khóa

Mục đích của KTC là cho phép vận chuyển khóa giữa một cặp thực thể (cả hai chia sẻ khóa với KTC).

Trong điều này, có 3 cơ chế thiết lập khóa sử dụng KTC được quy định. Trong mỗi cơ chế, một trong hai thực thể (bên khởi tạo) gửi đến KTC khóa K đã được mã hóa bằng khóa dùng chung giữa bên khởi tạo và KTC. KTC giải mã khóa K và tiến hành mã hóa lại bằng khóa dùng chung với thực thể thứ hai (tức là bên nhận cuối cùng) – quá trình cho kết quả là khóa chuyển. Sau đó KTC sẽ tiến hành :

a) Hoặc gửi khóa chuyển trở lại cho bên khởi tạo và từ đó chuyển tiếp khoá chuyển đến bên nhận cuối cùng,

b) Hoặc chuyển trực tiếp khóa chuyển cho bên nhận cuối cùng.

Để thực hiện các cơ chế được quy định trong điều này cần tuân thủ các yêu cầu sau:

a) Thực thể A và B chia sẻ khóa bí mật K_{AP} và K_{BP}, với bên thứ ba đáng tin cậy P (hoạt động như một KTC).

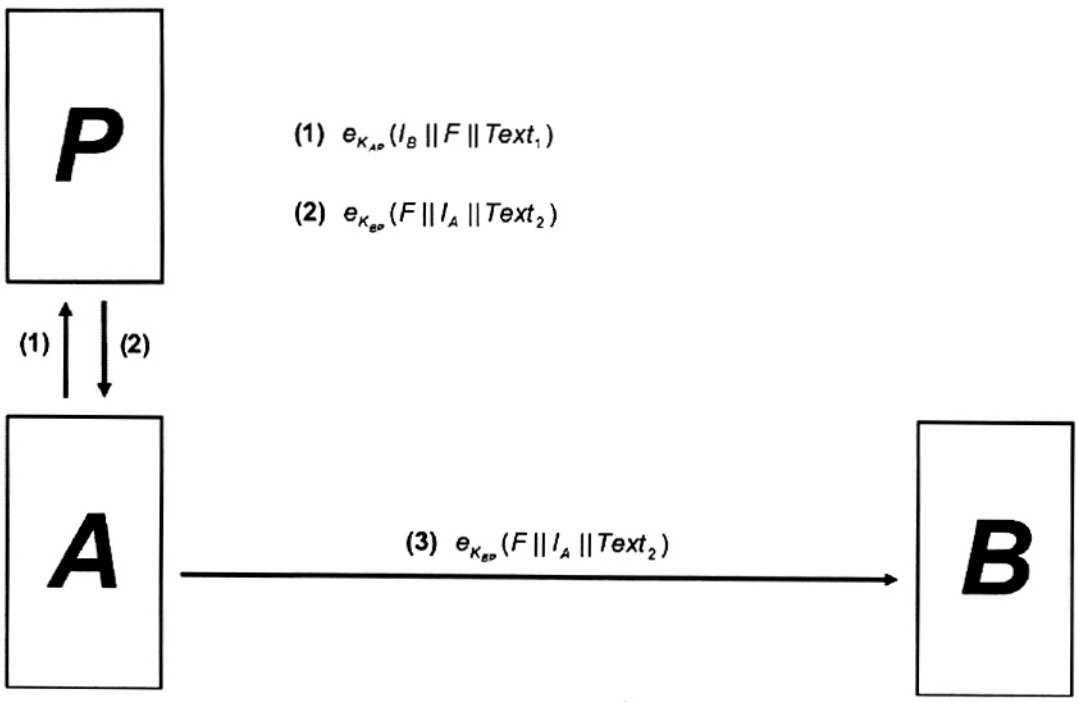
b) KTC phải có một phương pháp giao tiếp với thực thể yêu cầu chuyển khóa (bên khởi tạo).

c) Bên khởi tạo phải có khả năng tạo hoặc thu được bằng cách nào đó khóa K.

d) Các yêu cầu bảo mật liên quan tới tính bảo mật của khóa K và việc phát hiện sự thay đổi, sự thay thế hoặc sự phát lại các khóa và thông điệp.

8.1 Cơ chế thiết lập khóa 11

Trong cơ chế thiết lập khóa 11 thì khóa K được cung cấp bởi thực thể A.



Hình 11 – Cơ chế 11.

Cơ chế này bao gồm các bước sau (xem Hình 11):

1) A yêu cầu chuyển khóa bằng cách gửi thông điệp 1 đến KTC, bao gồm $e_{K_{AP}}(I_B \| F \| Text_1)$ mã hóa bằng khóa K_{AP}, trong đó gồm có định danh phân biệt I_B của thực thể B và vật liệu tạo khóa F (được làm từ khóa K với dữ liệu tùy chọn).

   i) Khi nhận được thông điệp 1, KTC giải mã và nhận được F, gắn thêm định danh phân biệt I_A và tiến hành mã hóa lại với K_{BP} để nhận được :

$$e_{K_{BP}}(F \| I_A \| Text_2).$$

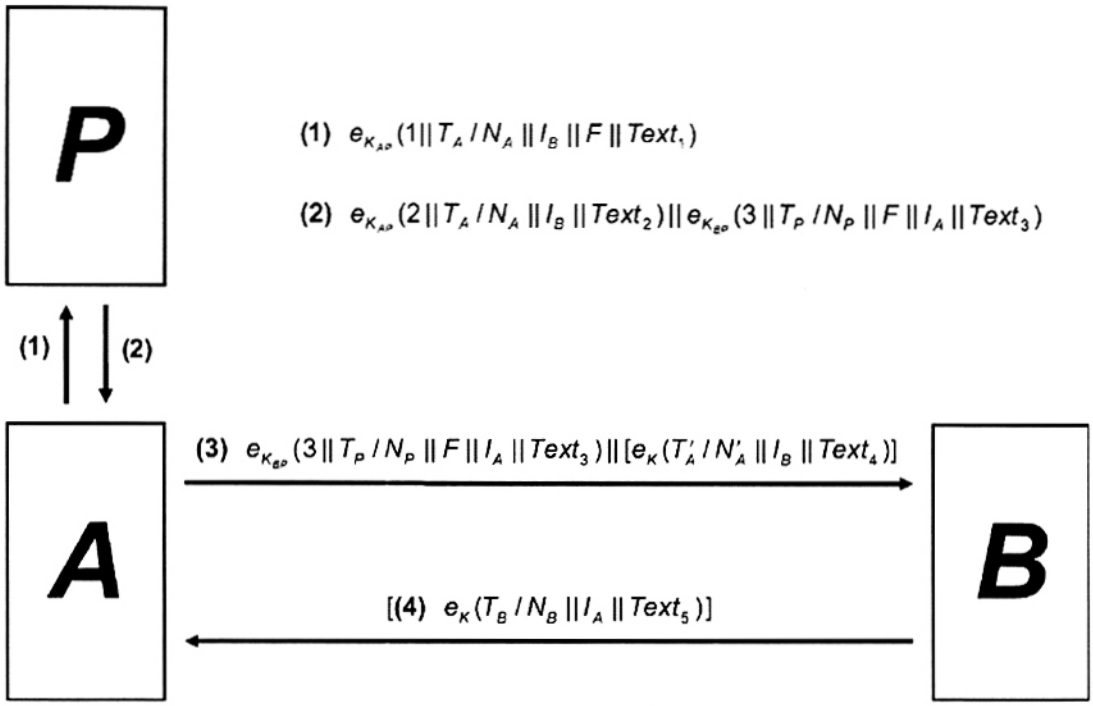
2) KTC gửi trả vật liệu khóa đã được mã hóa lại cho A trong thông điệp 2.

3) A chuyển tiếp $e_{K_{BP}}(F \| I_A \| Text_2)$ cho B trong thông điệp 3.

   i) Khi nhận được thông điệp 3, B giải mã phần mã hóa, kiểm tra tính đúng đắn của định danh phân biệt I_A và nhận được khóa K.

8.2 Cơ chế thiết lập khóa 12

Cơ chế thiết lập khóa 12 mặc dù được dẫn xuất từ cơ chế xác thực với 4 lần chuyển được quy định tại điều 6.1 trong ISO/IEC 9798 – 2:1999 nhưng không hoàn toàn tương thích với cơ chế đó. Trong cơ chế này khóa K được cung cấp bởi thực thể A. Tính duy nhất/ tính thời điểm được kiểm soát bởi tem thời gian hoặc số tuần tự. Cơ chế thiết lập khóa 12 có cung cấp tùy chọn xác thực hai chiều giữa A và B. Cơ chế này đòi hỏi cả A và B cùng KTC đều có khả năng duy trì các cơ chế để tạo ra hoặc xác minh tính hợp lệ của tem thời gian T hoặc số tuần tự N.



Hình 12 – Cơ chế 12.

Cơ chế này bao gồm các bước sau (xem Hình 12):

1) A yêu cầu chuyển khóa bằng cách gửi thông điệp 1 cho KTC, bao gồm số 1 và tem thời gian T_A hoặc số tuần tự N_A, định danh phân biệt I_B của B với vật liệu tạo khóa F (được làm từ khóa K với dữ liệu tùy chọn). Các trường dữ liệu được mã hóa bằng khóa K_{AP}.

   i) Khi nhận được thông điệp 1, KTC giải mã nó và kiểm tra sự hiện diện của số 1, kiểm tra tem thời gian T_A hoặc số tuần tự N_A và vật liệu tạo khóa đã mã hóa F.

2) KTC gửi thông điệp 2 cho A, chứa hai phần chính sau:

   – $e_{K_{AP}}(2 \| T_A / N_A \| I_B \| Text_2)$;

   – $e_{K_{BP}}(3 \| T_P / N_P \| F \| I_A \| Text_3)$.

i) Khi nhận được thông điệp 2, A giải mã phần thứ nhất, kiểm tra sự hiện diện của số 2 và định danh phân biệt I_B và tem thời gian T_A hoặc số tuần tự N_A (đã gửi cho KTC tại bước 1) có được dùng để kiến tạo thông điệp 2 hay không.

3) A chuyển tiếp phần hai của thông điệp 2 cho B bằng thông điệp 3,phần tùy chọn là phần thứ hai với trường dữ liệu:

$$e_K(T'_A / N'_A \| I_B \| Text_4);$$

trong đó kết hợp tem thời gian T'_A hoặc số tuần tự N'_A cho phép B kiểm tra tính toàn vẹn của khóa K thu được từ F.

i) Khi nhận được thông điệp 3, B giải mã phần thứ nhất, kiểm tra sự hiện diện của số 3 và định danh phân biệt I_A và nhận được khóa K.

ii) B giải mã phần thứ hai của thông điệp 3 (nếu có) và kiểm tra tem thời gian T'_A hoặc số tuần tự N'_A và sự hiện diện của định danh phân biệt I_B.

Bước thứ tư là tùy chọn, nó có thể được bỏ qua nếu không đòi hỏi xác thực thực thể hoặc xác thực một chiều. Bước 4 có thể được sử dụng nếu phần thứ hai của thông điệp 3 đã được gửi.

4) B gửi trả $e_K(T_B / N_B \| I_A \| Text_5)$ cho A trong thông điệp 4, qua đó xác nhận việc dùng chung khóa K.

i) Khi nhận được thông điệp 4, A giải mã và kiểm tra tem thời gian T_B hoặc số tuần tự N_B và sự hiện diện của định danh I_A .

CHÚ THÍCH 1 Thuật toán mã hóa e được sử dụng trong quá trình xác nhận khóa tùy chọn (tức là phần 2 của thông điệp 3 và thông điệp 4) có thể khác thuật toán mã hóa (cũng ký hiệu là e) được sử dụng để phân phối khóa.

CHÚ THÍCH 2 Để thực hiện xác thực hai chiều, cần có cả phần thông điệp tùy chọn tại bước 3 và bước 4.

8.3 Cơ chế thiết lập khóa 13

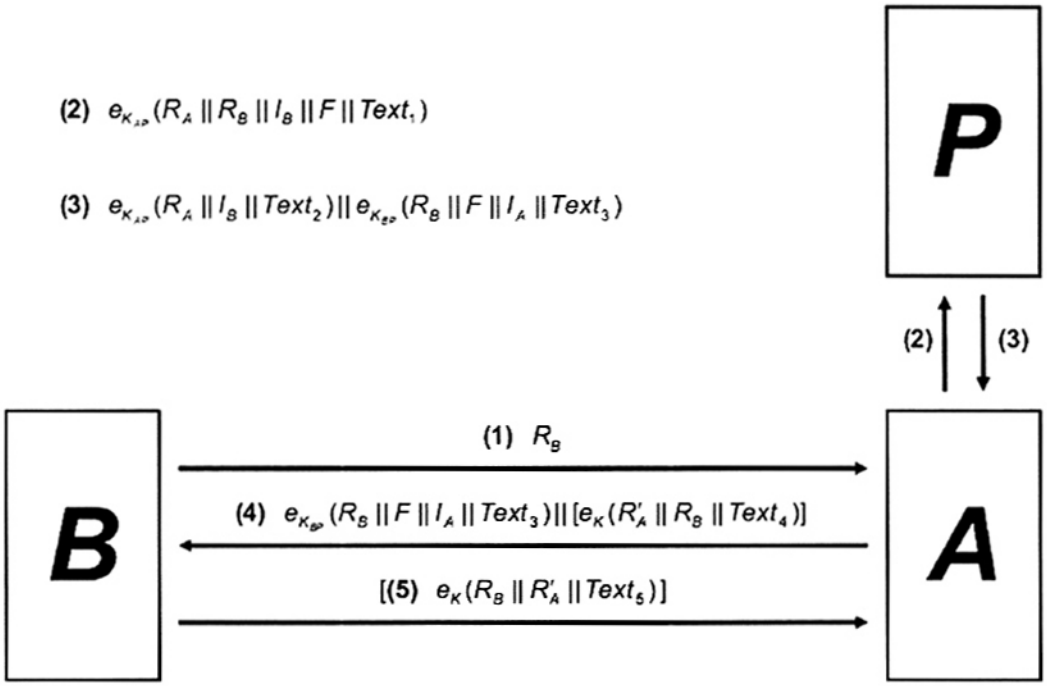
Cơ chế thiết lập khóa 13 mặc dù được dẫn xuất từ cơ chế xác thực với 5 lần chuyển được quy định tại điều 6.2 trong ISO/IEC 9798 – 2:1999 nhưng không hoàn toàn tương thích với cơ chế đó. Cơ chế thiết lập khóa 13 có cung cấp tùy chọn xác thực hai chiều giữa A và B. Tính duy nhất/ tính thời điểm được kiểm soát bởi số ngẫu nhiên. Cơ chế này đòi hỏi rằng A, B và KTC đều có khả năng tạo số ngẫu nhiên.

Cơ chế này bao gồm các bước sau (xem Hình 13):

1) B khởi tạo cơ chế bằng cách gửi số ngẫu nhiên R_B cho A trong thông điệp 1.

2) A yêu cầu chuyển khóa bằng cách gửi thông điệp 2 cho KTC bao gồm số ngẫu nhiên R_A và R_B cùng định danh phân biệt I_B và vật liệu tạo khóa F (được làm từ khóa K với dữ liệu tùy chọn). Các trường dữ liệu được mã hóa bằng khóa K_{AP}.

i) Khi nhận được thông điệp 2, KTC giải mã vật liệu tạo khóa đã mã hóa F và tiến hành mã hóa lại với các trường dữ liệu bổ xung (tùy chọn).



Hình 13 – Cơ chế 13.

3) KTC gửi thông điệp 3 cho A, bao gồm 2 phần chính:

- $e_{K_{AP}}(R_A \| I_B \| Text_2)$;
- $e_{K_{BP}}(R_B \| F \| I_A \| Text_2)$.

i) Khi nhận được thông điệp 3, A giải mã phần thứ nhất và kiểm tra định danh phân biệt I_B và số ngẫu nhiên R_A (đã được gửi cho KTC trong bước 2) có được sử dụng để tạo phần đầu của thông điệp 3 hay không.

4) A chuyển tiếp phần thứ hai của thông điệp 3 cho B trong thông điệp 4. Thông điệp 4 có thể chứa phần thứ hai tùy chọn là trường dữ liệu:

$$e_K(R'_A \| R_B \| Text_4)$$

đây là kết hợp của các số ngẫu nhiên R_B và R'_A và cho phép B kiểm tra được tính toàn vẹn của khóa K thu được từ F.

i) Khi nhận được thông điệp 4, B giải mã phần thứ nhất, kiểm tra định danh phân biệt I_A và số ngẫu nhiên R_B (đã gửi cho A trong bước 1) có được dùng để tạo nên phần thứ nhất của thông điệp 4 hay không, kiểm tra tính đúng đắn của định danh phân biệt I_A và thu được khóa K.

ii) B giải mã phần thứ hai của thông điệp 4 (nếu có) và kiểm tra số ngẫu nhiên R_B (đã gửi cho A ở bước 1 và đã được sử dụng để tạo thông điệp 4).

Bước thứ năm là tùy chọn, nó có thể được bỏ qua nếu không đòi hỏi xác thực thực thể hoặc chỉ xác thực một chiều. Bước 5 có thể được sử dụng nếu phần thứ hai của thông điệp 4 đã được gửi.

5) B gửi trả $e_K(R_B \| R'_A \| Text_5)$ cho A trong thông điệp 5, qua đó xác nhận việc dùng chung khóa K.

i) Khi nhận được thông điệp 5, A giải mã và kiểm tra số ngẫu nhiên R_B và R'_A (đã gửi cho B trong bước 4 và đã được sử dụng để tạo thông điệp 5).

CHÚ THÍCH 1 Thuật toán mã hóa e được sử dụng trong quá trình xác nhận khóa tùy chọn (tức là phần 2 của thông điệp 4 và thông điệp 5) có thể khác thuật toán mã hóa (cũng ký hiệu là e) được sử dụng để phân phối khóa.

CHÚ THÍCH 2 Để thực hiện xác thực hai chiều cần bao gồm cả phần thông điệp tùy chọn tại bước 4 và bước 5.

Phụ lục A

(quy định)

Mô đun ASN.1

A.1 Định nghĩa thủ tục

```
KeyManagementSymmetricTechniques {
        iso(1) standard(0) key–management(11770) part(2) asn1–module(0)
                key–management–mechanisms(0) }
DEFINITIONS EXPLICIT TAGS ::= BEGIN
                                        — IMPORTS None; —
OID ::= OBJECT IDENTIFIER
KeyEstablishmentMechanism ALGORITHM ::= {
 ke–mechanism1 |
 ke–mechanism2 |
 ke–mechanism3 |
 ke–mechanism4 |
 ke–mechanism5 |
 ke–mechanism6 |
 ke–mechanism7 |
 ke–mechanism8 |
 ke–mechanism9 |
 ke–mechanism10 |
 ke–mechanism11 |
 ke–mechanism12 |
 ke–mechanism13
}
                                            — Synonyms —
is11770–2 OID ::= { iso(1) standard(0) key–management(11770) part2(2) }
mechanism OID ::= { is11770–2 mechanisms(1) }
                                    — Point–to–point key establishment —
ke–mechanism1 OID ::= { mechanism 1 }
ke–mechanism2 OID ::= { mechanism 2 }
ke–mechanism3 OID ::= { mechanism 3 }
ke–mechanism4 OID ::= { mechanism 4 }
ke–mechanism5 OID ::= { mechanism 5 }
ke–mechanism6 OID ::= { mechanism 6 }
                                — Mechanisms using a key distribution centre –
ke–mechanism7 OID ::= { mechanism 7 }
ke–mechanism8 OID ::= { mechanism 8 }
ke–mechanism9 OID ::= { mechanism 9 }
ke–mechanism10 OID ::= { mechanism 10 }
                                — Mechanisms using a key translation centre –
ke–mechanism11 OID ::= { mechanism 11 }
ke–mechanism12 OID ::= { mechanism 12 }
ke–mechanism13 OID ::= { mechanism 13 }
                               END — KeyManagementSymmetricTechniques –
```

A.2 Sử dụng định danh đối tượng tiếp theo

Mỗi một cơ chế xác thực sử dụng hoặc thuật toán mã hóa hoặc hàm tạo khóa (hoặc cả hai) và bất kỳ tham số liên quan. Vì vậy, định danh đối tượng của cơ chế xác thực có thể tuân theo một trong số các định danh thuật toán của cơ chế mã hóa xác thực đã được quy định trong ISO/IEC 19772 và bất kỳ tham số liên quan.

Phụ lục B

(tham khảo)

Các đặc tính của cơ chế thiết lập khóa

Bảng B.1 tổng kết các đặc tính của các cơ chế thiết lập khóa được quy định trong tiêu chuẩn này. Các tùy chọn được biểu diễn trong dấu ngoặc vuông, ví dụ như cơ chế 8 có tùy chọn 4 lần chuyển để đạt được xác thực hai chiều. Các số mũ được chú thích ở phần tiếp theo sau bảng.

Bảng B.1 – Các đặc tính của cơ chế

Cơ chế	Bên thứ 3	Số lần chuyển	Kiểm soát khóa	Xác thực khóa[2]	Phát hiện phát lại[3]	Xác nhận khóa[4]	Xác thực thực thể[5]	Tính phức tạp[6]
1	–	1	A[1]	không	không	không	không	A: 1K B: 1K
2	–	1	A	không	không	không	không	A: 1E B: 1E
3	–	1	A	có	T/N	không	A	A: 1E B: 1E
4	–	2	A	có	R	không	A	A: 1E B: 1E
5	–	2	A/B	có	T/N	không	A&B	A: 1K+2E B: 1K+2E
6	–	3	A/B	có	R	không	A&B	A: 1K+2E B: 1K+2E
7	KDC	3	KDC	không	không	không	không	A: 1E B: 1E P: 2E
8	KDC	3[4]	KDC	có	T/N	tùy chọn	tùy chọn	A: 1E [3E] B: 1E [3E] P: 2E
9	KDC	4[5]	KDC	có	R	tùy chọn	tùy chọn	A: 1E [3E B: 1E [3E P: 2E
10	KDC	3	KDC	có	T/N	không	không	A: 2E B: 1E P: 3E
11	KTC	3	A	có	không	không	không	A: 1E B: 1E P: 2E
12	KTC	3[4]	A	có	T/N	tùy chọn	tùy chọn	A: 2E [4E] B: 1E [3E] P: 3E
13	KTC	4[5]	A	có	R	tùy chọn	tùy chọn	A: 2E [4E] B: 1E [3E] P: 3E

CHÚ THÍCH 1 Trong cơ chế 1, khóa K không trực tiếp được cung cấp bởi thực thể A nhưng dẫn xuất từ TVP do thực thể A cung cấp.

CHÚ THÍCH 2 Xác thực khóa ở đây là xác thực khóa tường minh. Tất cả các cơ chế đều yêu cầu ít nhất có xác thực khóa không tường minh, bởi vì chỉ các bên tham gia mới biết rõ khóa bí mật và có thể phục hồi khóa đã thiết lập bằng cơ chế đó. Tuy nhiên, cũng lưu ý rằng xác thực khóa tường minh không đảm bảo rằng khóa đã thiết lập là "tươi" (fresh), tức là không phải là lặp lại của khóa "cũ" – để đạt được "tính tươi" của khóa (freshness), đòi hỏi phải phát hiện ra sự lặp lại khóa.

CHÚ THÍCH 3 T/N chỉ ra cơ chế phát hiện lặp lại sử dụng tem thời gian hoặc số tuần tự và R chỉ ra cơ chế phát hiện lặp lại sử dụng số ngẫu nhiên.

CHÚ THÍCH 4 Xác nhận khóa có thể là "tùy chọn", chỉ ra cơ chế sử dụng kỹ thuật đã quy định trong Phụ lục C.

CHÚ THÍCH 5 Xác thực thực thể ở đây là xác thực giữa A và B. Đối với một số cơ chế trong Điều 7 và 8, xác thực một chiều hoặc lẫn nhau là tùy chọn.

CHÚ THÍCH 6 Tính phức tạp ở đây đề cập đến số lượng các thao tác mật mã được thực hiện bởi mỗi thực thể. Đằng sau tên của các thực thể (A, B, P) là số lượng các ứng dụng được yêu cầu cho hàm tạo khóa (K) và/hoặc hàm mã hóa/giải mã (E) được liệt kê. Các con số trong dấu ngoặc vuông cho thấy tính phức tạp nếu tất cả các bước tùy chọn được thực hiện (còn không là các bước tùy chọn không được thực hiện).

Định danh phân biệt chứa trong phần mã hóa của thông điệp tại một số cơ chế với mục đích là chống các kiểu tấn công dạng thay thế, tức là tái sử dụng bất hợp pháp các thông điệp được gửi bởi A hoặc B bằng một bên thứ ba giả mạo A hoặc B. Cụ thể hơn, trong một số trường hợp các định danh phân biệt được dùng để chống lại kiểu tấn công phản xạ (một hình thức cụ thể của kiểu tấn công dạng thay thế), khi mà thông điệp được gửi từ thực thể A tới thực thể B (và ngược lại) bị gửi ngược trở lại cho thực thể A bởi bên thứ ba giả mạo để thuyết phục A rằng nó đang giao tiếp với B. Trong trường hợp mà kiểu tấn công này không thể xảy ra, định danh phân biệt có thể được bỏ qua. Trường hợp đặc biệt mà kiểu tấn công phản xạ không thể xảy ra là khi hai thực thể A và B chia sẻ hai khóa bí mật khác nhau (khóa một chiều) được sử dụng riêng cho các thông điệp được gửi từ A tới B và các thông điệp được gửi từ B đến A.

Để biết thêm chi tiết về các kiểu tấn công như vậy và các biện pháp đối phó, xem thêm ví dụ [10] và [11] (tài liệu tham khảo).

Phụ lục C

(tham khảo)

Kỹ thuật phụ trợ

C.1 Tính toàn vẹn dữ liệu

C.1.1 Tính toàn vẹn của các thông điệp riêng lẻ

Trong các cơ chế thiết lập khóa được quy định trong tiêu chuẩn này, các trường dữ liệu được sử dụng để đảo bảm tính toàn vẹn của dữ liệu. Nếu hàm băm được sử dụng với mục đính đó, thì mã băm hoặc được gắn với dữ liệu trước khi mã hóa hoặc được đặt vào trong trường bản rõ. Nếu mã xác thực thông điệp được sử dụng, thì mã MAC phải được tính toán với thiết lập khóa phụ (riêng biệt) bằng cùng cơ chế. Trong mọi trường hợp, bên nhận K phải kiểm tra tính toàn vẹn của thông điệp và khóa đã nhận.

Cụ thể hơn, nếu hàm băm h được sử dụng để đảm bảo tính toàn vẹn dữ liệu của thông điệp

$$e_{K_{AB}}(...\|K\|Text\,1)$$

sau đó trường Text1 có thể coi là:

trong đó h(X) biểu thị hàm băm tính toán dữ liệu X. Ngoài ra nếu hàm MAC được dùng để đảm bảo tính toàn vẹn dữ liệu của thông điệp, thì trường bản rõ phải là:

$$Text\,1^*\|h(...\|K\|Text\,1^*)$$

$$MAC_{K^*}(e_{K_{AB}}(...\|K\|Text\,1))$$

sau đó có thể gắn vào thông điệp, trong đó K^* là khóa riêng từ K.

Tuy nhiên, khuyến khích sử dụng chế độ mã hóa xác thực (như đã chuẩn hóa trong ISO/IEC 19772) để kiến tạo e khi không có một cơ chế toàn vẹn riêng.

C.1.2 Tính toàn vẹn của hai phần thông điệp

Khi hai trường dữ liệu được mã hóa và ghép với nhau được gửi trả bởi KDC hoặc KTC (như trong cơ chế 7, 8, 9, 12 và 13) và các giả thiết a)1) và a)2) của Điều 5 không phải lúc nào cũng tương đương. Giả thiết a)1) chỉ có thể đảo bảo tính toàn vẹn của hai phần riêng lẻ, trong khi giả thiết a)2) lại có thể đảo bảo tính toàn vẹn của thông điệp một cách tổng thể. Trong trường hợp thứ hai, nó có thể phát hiện rõ ràng các liên kết trên các cuộc tấn công đang được thực hiện.

Xem ví dụ sau, chú ý cơ chế có thông điệp dạng :

$$e_{K_{AP}}(X)\|e_{K_{BP}}(Y)$$

là được gửi từ bên thứ ba đáng tin cậy P đến A để phát hiện một thay đổi bất kỳ của thông điệp trong khi chuyển giao giữa P và A, trường bản rõ có dạng:

$$MAC_{K^{\bullet}_{AP}}(e_{K_{AP}}(X) \| e_{K_{BP}}(Y) \| MAC_{K^{\bullet}_{BP}}(e_{K_{BP}}(Y))$$

có thể được gắn kết với thông điệp, trong đó $K^{\bullet}_{AP}$ và $K^{\bullet}_{BP}$ là biểu diễn khóa từ K_{AP} và K_{BP}.

C.2 Tính toán khóa

Tính toán khóa là kỹ thuật nhằm có được khóa từ hai hay nhiều khoản dữ liệu, ít nhất một trong số đó là bí mật, bằng cách sử dụng hàm tạo khóa f (có thể công khai). Ví dụ sau về hàm:

a) Các tổng mô đun 2 bit đảo của hai khoản dữ liệu mật F_1 và F_2 , tức là:

$$K = f(F_1, F_2) = F_1 \oplus F_2.$$

b) Áp dụng hàm băm h đã được định nghĩa trong ISO/IEC 10118 vào kết quả ghép hai khoản dữ liệu F_1 và F_2 , tức là:

$$K = f(F_1, F_2) = h(F_1 \| F_2).$$

Trong một số trường hợp, tốt nhất hàm tạo khóa là hàm một chiều, tức là có thông tin nhất định về đầu ra thì không thể tính toán được thông tin liên quan đến các tham số đầu vào bí mật. Lưu ý rằng, ví dụ hàm a) nói trên không phải là một chiều theo nghĩa này, từ thông tin về đầu ra K có thể biết lập tức thông tin hữu ích về tham số đầu vào bí mật F_1 và F_2. Trong cơ chế thiết lập khóa 1, điều cần thiết là các hàm tạo khóa f phải có tính một chiều, do đó nếu khóa K đã được thiết lập bằng cách dùng cơ chế này bị hỏng, thì khóa dùng chung bí mật K_{AB} (có thể được dùng "lâu dài") không bị hỏng.

Xem thêm thông tin về hàm khóa nguồn được tiếp nhận từ NIST SP 800 – 57 Phần 1, mục 8.2.4.

C.3 Xác nhận khóa

Xác nhận khóa là đặc tính theo đó một thực thể được đảm bảo rằng thực thể đã định danh còn lại có quyền sở hữu khóa đúng. Ví dụ như cách thực thể X phải cung cấp xác nhận khóa cho thực thể Y liên quan đến khóa K, là để cho phép X gửi thông điệp cho Y

$$e_K(TVP \| Text)$$

trong đó TVP là tham số tem thời gian có thể được xác minh bởi thực thể Y.

C.4 Kết hợp giữa thiết lập khóa và xác thực thực thể

Để cung cấp xác thực thực thể, các cơ chế thiết lập khóa trong tiêu chuẩn này có thể được kết hợp với cơ chế xác thực thực thể đã quy định trong ISO/IEC 9798 – 2 hoặc ISO/IEC 9798 – 4. Ví dụ dưới đây cho thấy kết quả nếu sự kết hợp của cơ chế thiết lập khóa 1 cùng cơ chế xác thực một chiều với 2 lần chuyển xác định tại Điều 5.1.2 của ISO/IEC 9798 – 4:1999.

Cơ chế này bao gồm các bước sau:

1) B tạo ra số ngẫu nhiên R_B và chuyển cho A trong thông điệp 1.

$$K = v_{K_{AB}}(R_B).$$

i) Cả hai A và B nhận được khóa K từ R_B khi sử dụng hàm MAC là v với khóa K_{AB}.

2) A gửi trả cho B:

$$v_{K_{AB}}(R_B \| I_B).$$

trong thông điệp 2, tức là hàm MAC đã tính toán dựa trên số ngẫu nhiên R_B và định danh phân biệt I_B.

i) Khi nhận được thông điệp 2, B kiểm tra định danh phân biệt I_B và số ngẫu nhiên R_B.

Tài liệu tham khảo

[1] ISO 8732:1988, Banking – Key management (wholesale) *Ngành ngân hàng – Quản lý khóa (bán buôn)*;

[2] ISO/IEC 9797, Information technology – Security techniques – Message Authentication Codes (MACs) (*tất cả các phần), Công nghệ thông tin – Kỹ thuật an ninh – Mã xác thực thông điệp (MACs)*;

[3] ISO/IEC 9798, Information technology – Security techniques – Entity authentication (*tất cả các phần), Công nghệ thông tin – Kỹ thuật an ninh – Xác thực thực thể*;

[4] ISO/IEC 10116:2006, Information technology – Security techniques – Modes of operation for an n–bit block cipher (*Công nghệ thông tin – Kỹ thuật an ninh – Chế độ hoạt động của mật mã khối n–bít*);

[5] ISO/IEC 10118, Information technology – Security techniques – Hash–functions (*tất cả các phần), Công nghệ thông tin – Kỹ thuật an ninh – Các hàm băm*;

[6] ISO 11568–2:2005, Banking – Key management (retail) – Part 2: Symmetric ciphers, their key management and life cycle (*Ngành ngân hàng – Quản lý khóa (bán lẻ) – Phần 2: Mã hóa đối xứng – Vòng đời và quản lý khóa*);

[7] ISO/IEC 18031:2005, Information technology – Security techniques – Random bit generation (*Công nghệ thông tin – Kỹ thuật an ninh – Tạo bít ngẫu nhiên*);

[8] ISO/IEC 18033, Information technology – Security techniques – Encryption algorithms (*Công nghệ thông tin – Kỹ thuật an ninh – Thuật toán mã hóa*);

[9] ISO/IEC 19772, Information technology – Security techniques – Authenticated encryption (*Công nghệ thông tin – Kỹ thuật an ninh – Mật mã được xác thực*);

[10] BOYD, C. and MATHURIA, A. Protocols for Authentication and Key Establishment. Springer, 2003 (*Giao thức để xác thực và thiết lập khóa*);

[11] MENEZES, A., VAN OORSCHOT, P. and VANSTONE, S. Handbook of Applied Cryptography. CRC Press, 1997 (*Hướng dẫn về ứng dụng mật mã*).