*Kỷ yếu Hội nghị Quốc gia lần thứ X về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR), Đà Nẵng, ngày 17-18/08/2017*
*DOI: 10.15625/vap.2017.00030*

# GIAO THỨC TRAO ĐỔI KHÓA AN TOÀN CHO CÁC HỆ MẬT KHÓA ĐỐI XỨNG

**Lưu Hồng Dũng[1], Hồ Ngọc Duy[2], Tống Minh Đức[1], Bùi Thế Truyền[3], Đặng Hùng Việt[4]**

[1] Khoa CNTT, Học viện Kỹ thuật Quân sự, [2] Cục CNTT, Bộ QP,

[3] Viện CNMP, Học viện Kỹ thuật Quân sự, [4] Khoa ĐTVT, Học viện Kỹ thuật Mật mã

*luuhongdung@gmail.com, hoduy207@gmail.com, ductm75@gmail.com, buithetruyen@gmail.com, hungvietdtc@gmail.com*

***TÓM TẮT:*** *Bài báo đề xuất xây dựng giao thức thỏa thuận khóa an toàn cho các hệ mật mã khóa đối xứng phát triển từ giao thức Diffie - Hellman. Các giao thức mới đề xuất có ưu điểm là các khóa bí mật chia sẻ tạo ra được xác thực về nguồn gốc nên có thể chống lại các kiểu tấn công giả mạo rất hiệu quả.*

***Từ khóa:*** *Key Establishment, Key Agreement Protocols, Key Exchange Protocol, Key Transport Protocols.*

## I. ĐẶT VẤN ĐỀ

Trong các hệ mật mã khóa đối xứng, việc thiết lập một khóa bí mật chung (*Key Establishment*) cho cả bên gửi/mã hóa và bên nhận/giải mã là một vấn đề rất quan trọng và phức tạp, được thực hiện bằng các thuật toán/giao thức thỏa thuận khóa (*Key Agreement Protocols*) hay chuyển khóa (*Key Transport Protocols*) và thường được gọi chung là các sơ đồ phân phối khóa. Giao thức thỏa thuận khóa đầu tiên được đề xuất bởi W. Diffie và M. Hellman vào năm 1976 [1], ở đó mỗi bên tham gia sẽ tạo ra thông tin để thỏa thuận việc thiết lập 1 khóa bí mật dùng chung rồi trao đổi trực tiếp cho nhau, vì thế nó còn được gọi là giao thức trao đổi khóa (*Key Exchange Protocol*) Diffie-Hellman (DHKE). Với giao thức HDKE, không một kẻ thứ 3 nào có thể tính được khóa bí mật của 2 đối tượng tham gia trao đổi khóa nếu không giải được bài toán logarit rời rạc DLP (Discrete Logarithm Problem) [2]. Tuy nhiên, DHKE không có cơ chế xác thực giữa các đối tượng tham gia truyền thông, nên dễ dàng bởi một kẻ thứ 3 không mong muốn khi đối tượng này mạo danh một trong 2 đối tượng trao đổi khóa để thiết lập 1 khóa chung với đối tượng kia [3]. Một hướng nghiên cứu nhằm khắc phục nhược điểm trên đây của DHKE là tích hợp giao thức này với các thuật toán chữ ký số, đã có một số kết quả về hướng nghiên cứu này được công bố [4 - 7]. Các giao thức trao đổi khóa được phát triển theo hướng tích hợp chữ ký số có nhược điểm chung là chi phí tính toán và lưu lượng truyền thông giữa các đối tượng trong quá trình thiết lập khóa thường khá lớn.

Trong phần tiếp theo của bài báo, nhóm tác giả đề xuất xây dựng giao thức trao đổi khóa an toàn cho các hệ mật khóa đối xứng trên cơ sở phát triển giao thức Diffie-Hellman, giao thức mới đề xuất được xây dựng theo hướng không tích hợp với thuật toán chữ ký số nhằm nâng cao hiệu quả thực hiện trong các ứng dụng, mà vẫn có khả năng chống lại các dạng tấn công giả mạo đã biết trong thực tế tương tự như các giao thức trao đổi khóa được tích hợp chữ ký số.

## II. XÂY DỰNG GIAO THỨC ĐỔI KHÓA AN TOÀN CHO CÁC HỆ MẬT KHÓA ĐỐI XỨNG

### *A. Giao thức trao đổi khóa MTA 17.5- 03*

Giả thiết rằng 2 đối tượng tham gia truyền thông ở đây là A và B sử dụng một thuật toán mật mã khóa đối xứng (DES, AES,...) để mã hóa dữ liệu cần trao đổi với nhau, khi đó giao thức trao đổi khóa đề xuất ở đây (ký hiệu: MTA 17.5 - 03) được sử dụng để thiết lập một khóa bí mật chung/chia sẻ giữa A và B, bao gồm các thủ tục như sau:

Thủ tục hình thành tham số và khóa

Thủ tục bao gồm các bước như sau:

1 - Sinh 2 số nguyên tố lớn và mạnh: $p$ và $q$, sao cho: $q \mid (p-1)$ hay: $p = N \times q + 1$, với N là một số nguyên dương.

2 - Chọn $g = \alpha^{(p-1)/q} \bmod p$, là phần tử sinh có bậc $q$ của nhóm $Z_p^*$, ở đây: $\alpha \in Z_p^*$.

3 - Khóa riêng $x$ được hình thành bằng cách chọn số nguyên thỏa mãn: $1 < x < q$.

4 - Khóa công khai được tính theo công thức:

$$y = g^x \bmod p \tag{1.1}$$

5 - Chọn hàm băm an toàn $H : \{0,1\}^* \mapsto Z_n$ với: $q < n < p$

6 - Công khai các giá trị: $p, q, g, y$. Giữ bí mật: $x$.

**Chú thích:**

Khóa bí mật của A là $x_A$ và của B là: $x_B$. Khóa công khai của A và B tương ứng là: $y_A$ và $y_B$ được tính theo (1.1). Chú ý rằng, $y_A$ và $y_B$ cần phải được chứng thực bởi một CA (Certificate Authority) đáng tin cậy.

Thủ tục trao đổi khóa

Thủ tục để thiết lập một khóa bí mật chung cho phép A mã hóa thông tin, B giải mã thông tin hoặc ngược lại, bao gồm các bước như sau:

*Bước 1*: Được thực hiện bởi A

1 - Chọn ngẫu nhiên một giá trị $k_A$ thỏa mãn: $1 < k_A < q$, tính giá trị $R_A$ theo công thức:

$$R_A = g^{k_A} \bmod p \tag{1.2}$$

2 - Tính thành phần $S_A$ theo công thức:

$$S_A = (y_B)^{x_A} \bmod p \tag{1.3}$$

3 - Tính thành phần $E_A$ theo công thức:

$$E_A = H(R_A \| S_A) \tag{1.4}$$

4 - Gửi ( $R_A, E_A$ ) cho B.

*Bước 2*: Được thực hiện bởi B

1 - Tính thành phần $S_B$ theo công thức:

$$S_B = (y_A)^{x_B} \bmod p \tag{1.5}$$

2 - Tính giá trị $\overline{E}_A$ theo công thức:

$$\overline{E}_A = H(R_A \| S_B) \tag{1.6}$$

3 - Kiểm tra nếu: $\overline{E}_A \neq E_A$ thì kết thúc. Ngược lại, nếu: $\overline{E}_A = E_A$ thì khẳng định đối tượng tham gia trao đổi khóa là A (đối tượng sở hữu khóa $y_A$) và thực hiện các bước tiếp theo:

4 - Chọn ngẫu nhiên một giá trị $k_B$ thỏa mãn: $1 < k_B < q$, tính khóa bí mật chia sẻ với A theo:

$$K_{BA} = (R_A)^{k_B} \bmod p \tag{1.7}$$

5 - Tính giá trị $R_B$ theo công thức:

$$R_B = g^{k_B} \bmod p \tag{1.8}$$

6 - Tính thành phần $E_B$ theo công thức:

$$E_{BA} = H(R_A \| R_B \| S_B) \tag{1.9}$$

7 - Gửi ( $R_B, E_{BA}$ ) cho A.

*Bước 3*: Được thực hiện bởi A

1 - Tính giá trị $\overline{E}_{BA}$ theo công thức:

$$\overline{E}_{BA} = H(R_A \| R_B \| S_A) \tag{1.10}$$

2 - Kiểm tra nếu: $\overline{E}_{BA} \neq E_{BA}$ thì kết thúc. Ngược lại, nếu: $\overline{E}_{BA} = E_{BA}$ thì khẳng định đối tượng tham gia trao đổi khóa là B (đối tượng sở hữu khóa $y_B$) và B đã thiết lập được khóa bí mật chia sẻ, khi đó A sẽ thực hiện các bước tiếp theo:

3 - Tính khóa bí mật chia sẻ với B theo:

$$K_{AB} = (R_B)^{k_A} \bmod p \tag{1.11}$$

4 - Tính thành phần $E_{AB}$ theo công thức:

$$E_{AB} = H(R_B \| S_A) \tag{1.12}$$

5 - Gửi $E_{AB}$ cho B.

*Bước 4*: Được thực hiện bởi B.

1 - Tính giá trị $\overline{E}_{AB}$ theo công thức:

$$\overline{E}_{AB} = H(R_B \| S_B) \tag{1.13}$$

2 - Kiểm tra nếu: $\overline{E}_{AB} = E_{AB}$ thì khẳng định đối tượng A đã thiết lập được khóa bí mật chia sẻ với B.

**Chú thích:**

- Khóa bí mật chung của A và B: $K = K_{AB} = K_{BA}$.

- Toán tử "||" dùng trong (1.4), (1.6), (1.9), (1.10), (1.12) và (1.13) là phép nối ghép 2 xâu bit.

Tính đúng đắn của giao thức MTA 17.5 - 03

Điều cần chứng minh ở đây là: cho $p$, $q$ là 2 số nguyên tố thỏa mãn: $q \mid (p-1)$, $g = \alpha^{(p-1)/q} \bmod p$, $\alpha \in Z_p^*$, $H : \{0,1\}^* \mapsto Z_n$ với: $q < n < p$, $1 < x_A, x_B < q$, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$, $1 < k_A, k_B < q$, $R_A = g^{k_A} \bmod p$, $R_B = g^{k_B} \bmod p$, $S_A = (y_B)^{x_A} \bmod p$, $S_B = (y_A)^{x_B} \bmod p$, $E_A = H(R_A \| S_A)$, $E_{BA} = H(R_A \| R_B \| S_B)$, $E_{AB} = H(R_B \| S_A)$. Nếu: $\overline{E}_A = H(R_A \| S_B)$, $\overline{E}_{BA} = H(R_A \| R_B \| S_A)$, $K_{AB} = (R_B)^{k_A} \bmod p$, $K_{BA} = (R_A)^{k_B} \bmod p$, $\overline{E}_{AB} = H(R_B \| S_B)$ thì: $\overline{E}_A = E_A$, $\overline{E}_{BA} = E_{BA}$, $\overline{E}_{AB} = E_{AB}$ và $K_{AB} = K_{BA}$.

*Chứng minh*:

Thật vậy, từ (1.1) và (1.3) ta có:

$$S_A = (y_B)^{x_A} \bmod p = (g^{x_B} \bmod p)^{x_A} \bmod p = g^{x_A \cdot x_B} \bmod p \tag{1.14}$$

Tương tự, từ (1.1) và (1.5):

$$S_B = (y_A)^{x_B} \bmod p = (g^{x_A} \bmod p)^{x_B} \bmod p = g^{x_A \cdot x_B} \bmod p \tag{1.15}$$

Từ (1.14) và (1.15) suy ra:

$$S_A = S_B \tag{1.16}$$

Từ (1.4), (1.6) và (1.16) suy ra điều cần chứng minh thứ nhất:

$$\overline{E}_A = H(R_A \| S_B) = H(R_A \| S_A) = E_A$$

Từ (1.9), (1.10) và (1.16) ta có điều cần chứng minh thứ hai:

$$E_{BA} = H(R_A \| R_B \| S_B) = H(R_A \| R_B \| S_A) = \overline{E}_{BA}$$

Tương tự, từ (1.12) và (1.13) và (1.16) ta có điều cần chứng minh thứ ba:

$$E_{AB} = H(R_B \| S_A) = H(R_B \| S_B) = \overline{E}_{AB}$$

Từ (1.8) và (1.11) ta có:

$$K_{AB} = (R_B)^{k_A} \bmod p = (g^{k_B} \bmod p)^{k_A} \bmod p = g^{k_A \cdot k_B} \bmod p \tag{1.17}$$

Từ (1.2) và (1.7) ta lại có:

$$K_{BA} = (R_A)^{k_B} \bmod p = (g^{k_A} \bmod p)^{k_B} \bmod p = g^{k_A \cdot k_B} \bmod p \tag{1.18}$$

Từ (1.17) và (1.18) suy ra điều cần chứng minh thứ tư: $K_{AB} = K_{BA}$

Độ an toàn của giao thức MTA 17.5 - 03

Giao thức được đề xuất ở đây bảo đảm các tính chất của một giao thức trao đổi khóa an toàn:

- *Xác thực thực thể* (*entity authentication*): là tính chất cho phép 1 trong 2 đối tượng khẳng định chắc chắn về danh tính của đối tượng tham gia thiết lập khóa bí mật chia sẻ với mình. Trong giao thức này, B kiểm tra điều kiện: $\overline{E}_A = E_A$ để khẳng định danh tính của A, còn A kiểm tra điều kiện: $\overline{E}_{BA} = E_{BA}$ để xác thực danh tính của B.

- *Xác thực khóa hiện* (*explicit key authentication*): là khả năng xác thực khóa (key anthentication) và xác nhận khóa (key comfirmation). Trong đó xác thực khóa hay còn gọi là xác thực khóa ẩn (implicit key authentication) là khả năng mà 1 trong 2 đối tượng có thể khẳng định một cách chắc chắn rằng chỉ có đối tượng kia mới có thể tạo ra khóa bí mật chia sẻ với mình, còn xác nhận khóa là khả năng mà 1 trong 2 đối tượng có thể khẳng định đối tượng kia đã tạo được khóa bí mật chia sẻ với mình khi giao thức đã thực hiện xong. Ở giao thức mới đề xuất, điều kiện: $\overline{E}_{BA} = E_{BA}$ cho A biết B đã nhận được $R_A$, còn: $\overline{E}_{AB} = E_{AB}$ lại cho B biết A đã nhận được $R_B$. Từ đó, A có thể khẳng định B đã tạo được khóa bí mật chia sẻ với mình và B cũng khẳng định được điều tương tự với A. Hơn nữa, không một đối tượng nào ngoài A và B có thể tạo được khóa bí mật chia sẻ: $K = g^{k_A.k_B} \bmod p$ nếu không giải được bài toán logarit rời rạc.

- *Tính an toàn khóa đã biết* (*known - key security*): tính chất này bảo đảm rằng một đối tượng thứ 3 dù biết được một số khóa bí mật chia sẻ được thiết lập bởi A và B thì cũng không thể tính được các khóa khác đã được thiết lập bởi A và B. Ở giao thức mới đề xuất, khóa bí mật chia sẻ giữa A và B được tạo ra từ 2 giá trị ngẫu nhiên ( $k_A, k_B$ ) ở mỗi phiên tạo khóa, vì thế việc lộ một số khóa bí mật chia sẻ cũng không ảnh hưởng đến các khóa bí mật đã được tạo ra trước hoặc sau đó.

- *Tính bí mật về phía trước* (*forward secrecy*): tính chất này bảo đảm rằng việc lộ khóa bí mật của A hoặc B hoặc đồng thời cả 2 cũng không cho phép một đối tượng thứ 3 tính được các khóa bí mật chia sẻ đã được thiết lập trước đó bởi A và B.

Hiệu quả thực hiện của giao thức MTA 17.5 - 03

Hiệu quả thực hiện của các giao thức trao đổi khóa có thể được đánh giá thông qua số phép toán cần thực hiện hay tổng thời gian cần thực hiện các phép toán để thiết lập được khóa bí mật chia sẻ giữa 2 bên A và B. Để so sánh hiệu quả thực hiện của giao thức mới đề xuất với các giao thức trao đổi khóa có tích hợp chữ ký số [4-7], ở đây quy ước sử dụng các ký hiệu:

$T_{exp}$ : thời gian thực hiện một phép toán mũ modul;

$T_{inv}$ : thời gian thực hiện một phép toán mũ nghịch đảo modul;

$T_h$ : thời gian thực hiện hàm băm (*hash function*).

$T_{mul}$ : thời gian thực hiện một phép toán nhân modul;

*a) Thời gian thực hiện của giao thức Arazi* [4]*:*

Thời gian tính toán của bên A cho một lần thiết lập là:

Thời gian tính $(R_A, S_A)$ là: $(T_{exp} + T_h + T_{inv} + 2T_{mul})$

Thời gian thực hiện kiểm tra $(R_B, S_B)$: $(2T_{exp} + T_h + T_{inv} + 3T_{mul})$

Thời gian tính khóa *K* là: $(T_{exp})$

Tổng thời gian thực hiện: $\mathbf{(4T_{exp} + 2T_h + 2T_{inv} + 5T_{mul})}$

Bên B cần thời gian tương tự để hoàn thành giao thức, vậy thời gian tính toán cần thiết để hoàn thành giao thức là: $\mathbf{(8T_{exp} + 4T_h + 4T_{inv} + 10T_{mul})}$.

*b) Thời gian thực hiện của giao thức Harn* [5]*:*

Thời gian tính toán của bên A cho một lần thiết lập là:

Thời gian tính $(m_{A1}, m_{A2}, S_A)$ là: $(2T_{exp} + T_h + T_{inv} + 3T_{mul})$

Thời gian tính $r_B$ là: $(T_{mul})$

Thời gian thực hiện kiểm tra $(r_B, s_B)$: $(2T_{exp} + T_h + T_{inv} + 3T_{mul})$

Thời gian tính khóa $K_{AB1}$, $K_{AB2}$, $K_{AB3}$ là: $(3T_{exp})$

Tổng thời gian thực hiện: $\mathbf{(7T_{exp} + 2T_h + 2T_{inv} + 7T_{mul})}$

Bên B cần thời gian tương tự để hoàn thành giao thức, vậy thời gian tính toán cần thiết để hoàn thành giao thức là: $\mathbf{(14T_{exp} + 4T_h + 4T_{inv} + 14T_{mul})}$.

*c) Thời gian thực hiện của giao thức Phan* [6]*:*

Thời gian tính toán bước 1 của bên A là: $(2T_{exp})$

Thời gian tính toán bước 2 của bên B là: $(4T_{exp} + T_h + T_{inv} + 3T_{mul})$

Thời gian tính toán bước 3 của bên A là: $(4T_{exp} + 2T_h + 2T_{inv} + 6T_{mul})$

Thời gian tính toán bước 4 của bên B là: $(2T_{exp} + T_h + T_{inv} + 3T_{mul})$

Tổng thời gian thực hiện: $(\mathbf{10T_{exp} + 4T_h + 4T_{inv} + 12T_{mul}})$

*d) Thời gian thực hiện của giao thức 2 bước truyền trong [7] (MTA 16.6 - 01):*

Thời gian tính toán bước 1 của bên A là: $(T_{exp} + T_h + T_{inv} + T_{mul})$

Thời gian tính toán bước 2 của bên B là: $(4T_{exp} + 2T_h + 2T_{inv} + 2T_{mul})$

Thời gian tính toán bước 3 của bên A là: $(3T_{exp} + T_h + T_{inv} + T_{mul})$

Tổng thời gian thực hiện: $(\mathbf{8T_{exp} + 4T_h + 4T_{inv} + 4T_{mul}})$

*e) Thời gian thực hiện của giao thức 1 bước truyền trong [7] (MTA 16.6 - 02):*

Thời gian tính toán bước 1 của bên A là: $(2T_{exp} + T_h + T_{inv} + T_{mul})$

Thời gian tính toán bước 2 của bên B là: $(3T_{exp} + T_h + T_{inv} + T_{mul})$

Tổng thời gian thực hiện: $(\mathbf{5T_{exp} + 2T_h + 2T_{inv} + 2T_{mul}})$

*f) Thời gian thực hiện của giao thức MTA 17.5 - 03:*

Thời gian tính toán bước 1 của bên A là: $(2T_{exp} + T_h)$

Thời gian tính toán bước 2 của bên B là: $(3T_{exp} + 2T_h)$

Thời gian tính toán bước 3 của bên A là: $(T_{exp} + 2T_h)$

Thời gian tính toán bước 4 của bên B là: $(T_h)$

Tổng thời gian thực hiện: $(\mathbf{6T_{exp} + 6T_h})$

*g) Tổng hợp thời gian thực hiện của các giao thức:*

Tổng hợp thời gian thực hiện của giao thức mới đề xuất MTA 17.5 - 03 và của các giao thức trao đổi khóa tích hợp chữ ký số [4 - 7] được chỉ ra trên Bảng 1 như sau:

**Bảng 1.** Thời gian thực hiện của các giao thức

| TT | Tên giao thức | Tổng thời gian thực hiện |
|---|---|---|
| 1 | *Arazi* | $8T_{exp} + 4T_h + 4T_{inv} + 10T_{mul}$ |
| 2 | *Harn* | $14T_{exp} + 4T_h + 4T_{inv} + 14T_{mul}$ |
| 3 | *Phan* | $10T_{exp} + 4T_h + 4T_{inv} + 12T_{mul}$ |
| 4 | *MTA 16.6 - 01* | $8T_{exp} + 4T_h + 4T_{inv} + 4T_{mul}$ |
| 5 | *MTA 17.5 - 03* | $6T_{exp} + 6T_h$ |

Kết quả từ Bảng 1 cho thấy hiệu quả thực hiện của MTA 17.5 - 03 cao hơn các giao thức trao đổi khóa được thiết kế theo phương pháp tích hợp chữ ký số trong [4 - 7].

*Chú ý*: Giao thức 1 bước truyền dữ liệu trong [7] (ở đây ký hiệu MTA 16.6 - 02) có hiệu quả thực hiện cao hơn MTA 16.6 - 02 nhưng không bảo đảm được một số tính chất an toàn của giao thức trao đổi khóa và chỉ có thể ứng dụng rất hạn chế trong một số trường hợp cụ thể.

***B. Giao thức trao đổi khóa MTA 17.5- 04***

Giao thức trao đổi khóa đề xuất ở đây (ký hiệu: MTA 17.5 - 04) có sự cải tiến nhằm nâng cao hiệu quả thực hiện và lưu lượng truyền tin so với MTA 17.5- 03. Tuy nhiên điểm khác biệt chủ yếu giữa 2 giao thức này là ở chỗ: MTA 17.5 - 03 làm việc theo cơ chế tuần tự, còn MTA 17.5 - 04 lại có cơ chế làm việc theo kiểu song song. Nghĩa là việc trao đổi thông tin thiết lập khóa giữa A và B được thực hiện nối tiếp nhau ở MTA 17.5 - 03, còn ở MTA 17.5 - 04 các thông tin này được trao đổi đồng thời với nhau.

Tương tự giao thức MTA 17.5 - 03, ở đây cũng giả thiết rằng các đối tượng A và B thống nhất sử dụng một thuật toán mật mã khóa đối xứng (DES, AES,...) để mã hóa thông tin và thủ tục hình thành tham số - khóa cũng bao gồm các bước thực hiện tương tự ở Mục 2.1.1, khi đó thuật toán để thiết lập một khóa bí mật chung cho phép A và B trao đổi thông tin mật với nhau, bao gồm các thủ tục như sau:

Thủ tục trao đổi khóa

*Bước 1*:

+ Được thực hiện bởi A:

1 - Chọn ngẫu nhiên một giá trị $k_A$ thỏa mãn: $1 < k_A < q$, tính giá trị $R_A$ theo công thức:

$$R_A = g^{k_A} \bmod p \tag{2.1}$$

2 - Gửi $R_A$ cho B.

+ Được thực hiện bởi B:

1 - Chọn ngẫu nhiên một giá trị $k_B$ thỏa mãn: $1 < k_B < q$, tính giá trị $R_B$ theo công thức:

$$R_B = g^{k_B} \bmod p \tag{2.2}$$

2 - Gửi $R_B$ cho A.

*Bước 2*:

+ Được thực hiện bởi A:

1 - Tính thành phần $S_A$ theo công thức:

$$S_A = (y_B)^{x_A} \bmod p \tag{2.3}$$

2 - Tính khóa bí mật chia sẻ với B theo:

$$K_{AB} = (R_B)^{k_A} \bmod p \tag{2.4}$$

3 - Tính thành phần $E_A$ theo công thức:

$$E_A = H(K_{AB} \| S_A) \tag{2.5}$$

4 - Gửi $E_A$ cho B.

+ Được thực hiện bởi B:

1 - Tính thành phần $S_B$ theo công thức:

$$S_B = (y_A)^{x_B} \bmod p \tag{2.6}$$

2 - Tính khóa bí mật chia sẻ với A theo:

$$K_{BA} = (R_A)^{k_B} \bmod p \tag{2.7}$$

3 - Tính thành phần $E_B$ theo công thức:

$$E_B = H(K_{BA} \| S_B) \tag{2.8}$$

4 - Gửi $E_B$ cho A.

*Bước 3*:

+ Được thực hiện bởi A:

1 - Kiểm tra nếu: $E_A = E_B$ thì khẳng định đối tượng tham gia trao đổi khóa là B (đối tượng sở hữu khóa $y_B$) và B đã thiết lập được khóa bí mật chia sẻ với A.

2 - Kiểm tra nếu: $E_A \neq E_B$ thì khẳng định đối tượng tham gia trao đổi khóa không phải là B.

+ Được thực hiện bởi B:

1 - Kiểm tra nếu: $E_A = E_B$ thì khẳng định đối tượng tham gia trao đổi khóa là A (đối tượng sở hữu khóa $y_A$) và A đã thiết lập được khóa bí mật chia sẻ với B.

2 - Kiểm tra nếu: $E_A \neq E_B$ thì khẳng định đối tượng tham gia trao đổi khóa không phải là A.

Tính đúng đắn của giao thức MTA 17.5 - 04

Điều cần chứng minh ở đây là: cho $p$, $q$ là 2 số nguyên tố thỏa mãn: $q|(p-1)$, $g = \alpha^{(p-1)/q} \bmod p$, $\alpha \in Z_p^*$, $H: \{0,1\}^* \mapsto Z_n$ với: $q < n < p$, $1 < x_A, x_B < q$, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$, $1 < k_A, k_B < q$, $R_A = g^{k_A} \bmod p$, $R_B = g^{k_B} \bmod p$. Nếu: $S_A = (y_B)^{x_A} \bmod p$, $S_B = (y_A)^{x_B} \bmod p$, $K_{AB} = (R_B)^{k_A} \bmod p$, $E_A = H(K_{AB} \| S_A)$, $K_{BA} = (R_A)^{k_B} \bmod p$, $E_B = H(K_{BA} \| S_B)$ thì: $K_{AB} = K_{BA}$ và $E_A = E_B$.

*Chứng minh*:

Thật vậy, từ (2.2) và (2.4) ta có:

$$K_{AB} = (R_B)^{k_A} \bmod p = \left(g^{k_B} \bmod p\right)^{k_A} \bmod p = g^{k_A.k_B} \bmod p \quad (2.9)$$

Mặt khác, từ (2.1) và (2.7) ta lại có:

$$K_{BA} = (R_A)^{k_B} \bmod p = \left(g^{k_A} \bmod p\right)^{k_B} \bmod p = g^{k_A.k_B} \bmod p \quad (2.10)$$

Từ (2.9) và (2.10) suy ra điều cần chứng minh thứ nhất: $K_{AB} = K_{BA}$

Từ (1.1) và (2.3) ta có:

$$S_A = (y_B)^{x_A} \bmod p = \left(g^{x_B} \bmod p\right)^{x_A} \bmod p = g^{x_A.x_B} \bmod p \quad (2.11)$$

Từ (1.1) và (2.6) ta lại có:

$$S_B = (y_A)^{x_B} \bmod p = \left(g^{x_A} \bmod p\right)^{x_B} \bmod p = g^{x_A.x_B} \bmod p \quad (2.12)$$

Từ (2.11) và (2.12) suy ra:

$$S_A = S_B \quad (2.13)$$

Từ (2.5), (2.8) và (2.13) suy ra điều cần chứng minh thứ hai:

$E_A = H(K_{AB} \parallel S_A) = H(K_{BA} \parallel S_B) = E_B$

Độ an toàn của giao thức MTA 17.5 - 04

Tương tự MTA 17.5 - 03, giao thức được đề xuất cũng bảo đảm các tính chất của một giao thức trao đổi khóa an toàn:

- *Xác thực thực thể* (*entity authentication*): ở giao thức này việc kiểm tra điều kiện $E_A = E_B$ cho phép các đối tượng tham gia trao đổi khóa hoàn toàn có thể xác thực được danh tính của nhau.

- *Xác thực khóa hiện* (*explicit key authentication*): Cũng chỉ với việc kiểm tra điều kiện $E_A = E_B$, A hoàn toàn có thể khẳng định B đã tạo được khóa bí mật chia sẻ với mình và B cũng có thể khẳng định được điều tương tự như thế với A.

- *Tính an toàn khóa đã biết* (*known - key security*): tương tự MTA 17.5 - 03, việc biết một hoặc một số khóa chia sẻ giữa A và B cũng không cho phép một đối tượng thứ 3 nào đó có thể tính được các khóa khác cũng được thiết lập bởi A và B.

- *Tính bí mật về phía trước* (*forward secrecy*): việc tính các khóa bí mật chia sẻ đã được thiết lập trước đó bởi A và B là không thể thực hiện được, dù các khóa bí mật của A và B ( $x_A, x_B$ ) bị lộ.

Hiệu quả thực hiện của giao thức MTA 17.5 - 04

Thời gian cần thực hiện để thiết lập khóa bí mật chia sẻ giữa 2 bên A và B của giao thức mới đề xuất được tính toán như sau:

Thời gian tính toán bước 1 của bên A là: ($T_{exp}$)

Thời gian tính toán bước 1 của bên B là: ($T_{exp}$)

Thời gian tính toán bước 2 của bên A là: ($2T_{exp} + T_h$)

Thời gian tính toán bước 2 của bên B là: ($2T_{exp} + T_h$)

Tổng thời gian cần thực thực hiện để thiết lập khóa bí mật chia sẻ là: (**$6T_{exp} + 2T_h$**)

Từ đây có thể thấy rằng hiệu quả thực hiện xét theo khía cạnh chi phí tính toán để thiết lập khóa của giao thức MTA 17.5 - 04 là cao hơn MTA 17.5 - 03 và do đó cũng sẽ cao hơn các giao thức trao đổi khóa được tích hợp chữ ký số trong [4 - 7].

## III. KẾT LUẬN

Bài báo đề xuất 2 giao thức trao đổi khóa cho các hệ mật khóa đối xứng, các giao thức mới đề xuất có khả năng tạo ra khóa bí mật chia sẻ giữa 2 đối tượng được xác thực về nguồn gốc khóa, vì thế các giao thức này có khả năng chống được các dạng tấn công giả mạo đã biết trong thực tế tương tự như các giao thức trao đổi khóa được tích hợp chữ ký số, song lại có hiệu quả cao hơn về chi phí tính toán cần thực hiện trong quá trình thiết lập khóa.

## TÀI LIỆU THAM KHẢO

[1]. W. Diffie & M. Hellman, "*New Directions in Cryptography"*, IEEE Trans. On Info. Theory, IT-22(6):644-654, 1976.

[2]. T. ElGamal (1985), "*A public key cryptosystem and a signature scheme based on discrete logarithms*", IEEE Transactions on Information Theory. Vol. IT-31, No. 4. pp.469-472.

[3]. Mark Stamp, Richard M. Low, "*Applicd cryptanalysis: Breaking Ciphers in the Real World*", John Wiley & Sons, Inc., ISBN 978-0-470-1.

[4]. B. Arazi (1993), "*Integrating a key distribution procedure into the digital signature standard*", *Electronics Letters*, Vol. 29(11), pp.966-967.

[5]. L. Harn (1995), "*Modified key agreement protocol based on the digital signature standard*". Electronics Letters, Vol.31(6), pp. 448-449.

[6]. R. C. W. Phan (2005), "*Fixing the integrated Diffie-Hellman DSA key exchange protocol*", IEEE CommunicationLetters, Vol.9(6), pp. 570-572.

[7]. Hoàng Văn Việt, Bùi Thế Truyền, Tống Minh Đức, Lưu Hồng Dũng (06/2016), "*Thuật toán thỏa thuận khóa an toàn cho hệ mật khóa đối xứng*", Chuyên san CNTT và truyền thông/Tạp chí Khoa học và Kỹ thuật - Học viện KTQS. Số 8, trang 52-62. ISSN: 1859 - 0209.

# THE KEY EXCHANGE PROTOCOLS FOR SYMMETRIC - KEY CRYPTOSYSTEMS

**Luu Hong Dung, Ho Ngoc Duy, Tong Minh Duc, Bui The Truyen, Dang Hung Viet**

***ABSTRACT:*** *This paper proposes two new key exchange protocols for symmetric - key cryptosystems. The new proposed protocols has the ability to validate the origin of the shared secret key.*

***Keywords:*** *Key Establishment, Key Agreement Protocols, Key Exchange Protocol, Key Transport Protocols.*