

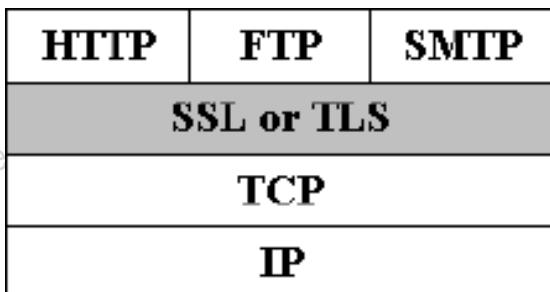
| | | |
|---|--|-----------------|
|  | VIETTEL AI RACE | TD163 |
| | MỘT SỐ GIAO THỨC ĐẢM BẢO ATTT DỰA TRÊN MÃ HÓA | Lần ban hành: 1 |

1. SSL/TLS

1.1 Giới thiệu

SSL (Secure Socket Layer) là giao thức bảo mật do công ty Netscape phát minh năm 1993. Các phiên bản SSL được phát triển bao gồm: phiên bản 1.0 phát hành năm 1993, phiên bản 2.0 phát hành năm 1995 và phiên bản 3.0 phát hành năm 1996. Sau phiên bản 3.0, SSL chính thức dừng phát triển. SSL hiện ít được sử dụng do có nhiều lỗi và không được cập nhật.

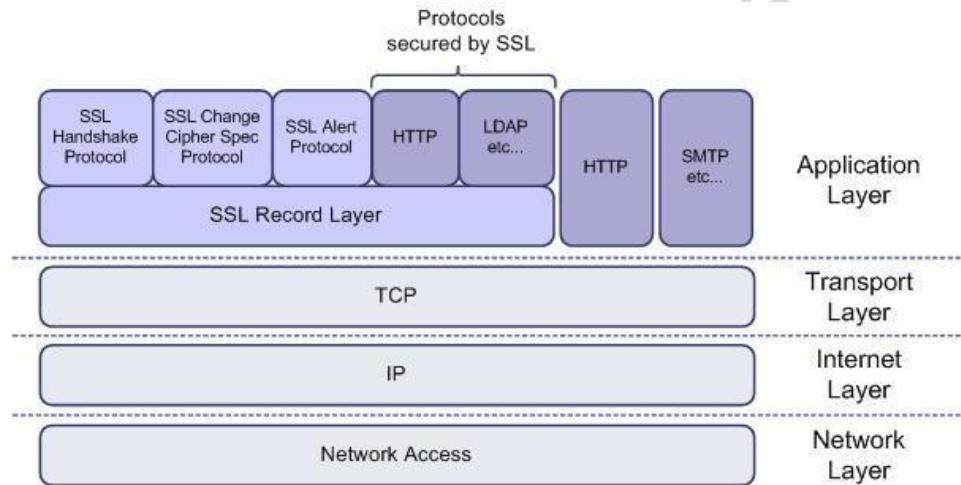
TLS (Transport Layer Security) được phát triển vào năm 1999 dựa trên SSL 3.0 do tổ chức IETF phê chuẩn. Các phiên bản của TLS gồm: phiên bản 1.0 phát hành năm 1999, phiên bản 1.1 phát hành năm 2005, phiên bản 1.2 phát hành năm 2008, phiên bản 1.3 vẫn là bản thảo và chưa được phát hành chính thức cho đến tháng 10 năm 2017. Hiện nay phiên bản TLS 1.2 được sử dụng rộng rãi nhất, còn SSL chỉ được giữ lại tên với lý do lịch sử.



Hình 3.41. SSL/TLS trong bộ giao thức TCP/IP

Hình 3.41 biểu diễn vị trí của giao thức SSL/TLS trong chồng giao thức TCP/IP. Có thể thấy SSL/TLS hoàn toàn độc lập với các giao thức tầng ứng dụng nên nó có thể được sử dụng để bảo mật thông tin truyền cho nhiều giao thức ứng dụng khác nhau, như HTTP, SMTP và FTP. Chẳng hạn, giao thức bảo mật web HTTPS = HTTP + SSL/TLS, có nghĩa là HTTPS tạo ra bởi HTTP chạy trên nền SSL/TLS. Một trong các điều kiện để SSL/TLS có thể hoạt động là ít nhất một thực thể (thường là máy chủ) tham gia phiên truyền thông phải có chứng chỉ số cho khóa công khai (Public key certificate).

| | | |
|---|--|-----------------|
|  | VIETTEL AI RACE MỘT SỐ GIAO THỨC ĐẢM BẢO ATTT DỰA TRÊN MÃ HÓA | TD163 |
| | | Lần ban hành: 1 |

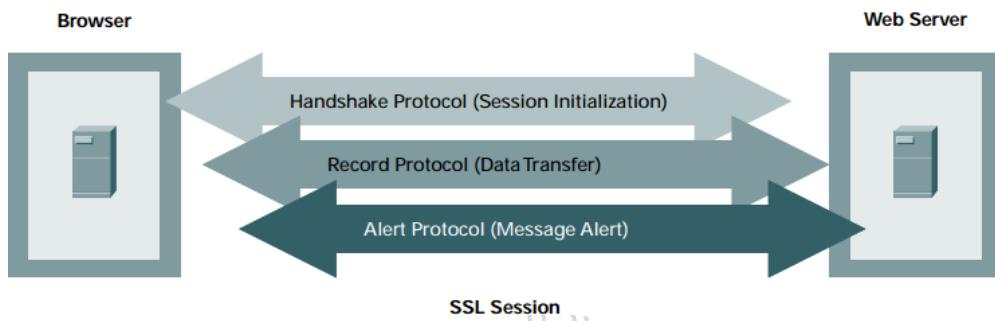


Hình 3.42. Các giao thức con của SSL/TLS

SSL/TLS là một bộ gồm có 4 giao thức con, như minh họa trên Hình 3.42. Các giao thức con của SSL/TLS gồm:

- SSL Handshake Protocol: Giao thức bắt tay của SSL có nhiệm vụ trao đổi các thông điệp xác thực thực thể và thiết lập các thông số cho phiên làm việc;
- SSL Change Cipher Spec Protocol: Giao thức thiết lập việc sử dụng các bộ mã hóa được hỗ trợ bởi cả 2 bên tham gia phiên truyền thông;
- SSL Alert Protocol: Giao thức cảnh báo của SSL;
- SSL Record Protocol: Giao thức bản ghi của SSL có nhiệm vụ tạo đường hầm an toàn để chuyển thông tin đảm bảo tín bí mật, toàn vẹn và xác thực.

1.2 Hoạt động của SSL/TS



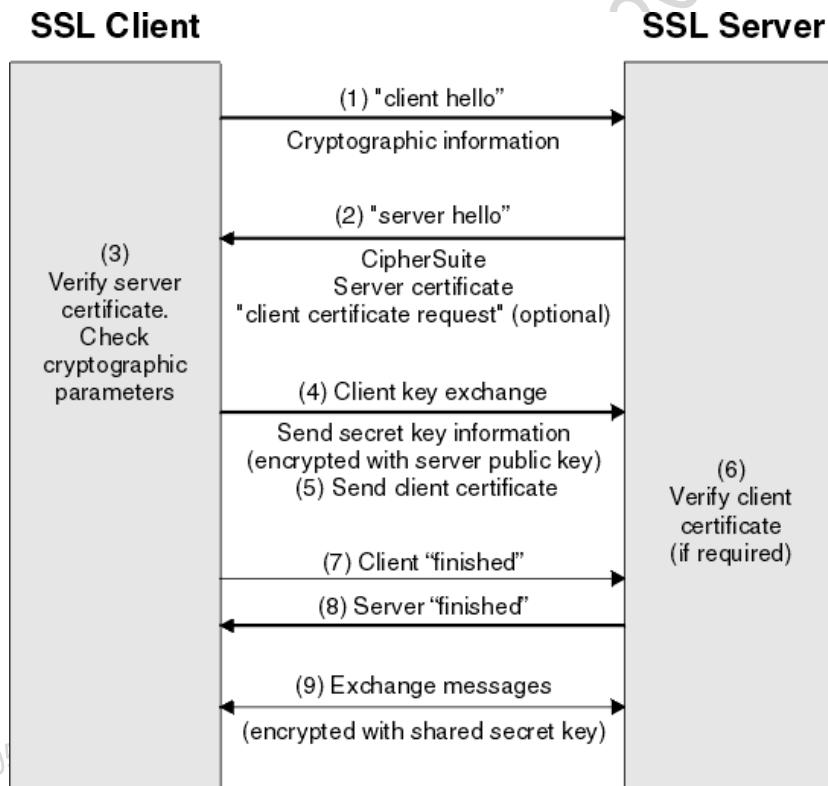
Hình 3.43. Mô hình truyền thông giữa Web Server và Browser dựa trên SSL/TLS

Hình 3.43 biểu diễn mô hình một phiên truyền thông giữa máy chủ web (Web Server) và máy khách web (Browser) dựa trên SSL/TLS. Theo đó, giao thức Bắt tay (Handshake) khởi tạo phiên làm việc (có sự hỗ trợ của giao thức Change Cipher Spec), giao thức Bản ghi (Record) vận chuyển dữ liệu an toàn và giao

| | | |
|---|--|-----------------|
|  | VIETTEL AI RACE MỘT SỐ GIAO THỨC ĐÀM BẢO ATTT DỰA TRÊN MÃ HÓA | TD163 |
| | | Lần ban hành: 1 |

thức Cảnh báo (Alert) gửi các cảnh báo khi xảy ra lỗi, hoặc một sự kiện đặc biệt.

1.2.1 Khởi tạo phiên làm việc



Hình 3.44. Khởi tạo phiên làm việc trong SSL/TLS

Quá trình khởi tạo phiên làm việc trong SSL/TLS được thực hiện bởi giao thức SSL Handshake với sự hỗ trợ của giao thức SSL Change Cipher Spec. Các nhiệm vụ được các

bên tham gia truyền thông thực hiện trong quá trình này bao gồm: (1) xác thực thông tin nhận dạng, (2) đàm phán thống nhất các bộ mã hóa sử dụng và (3) trao đổi khóa và các thông số khác cho phiên truyền thông.

Quá trình khởi tạo phiên làm việc biểu diễn trên Hình 3.44 giữa SSL Client (máy khách) và SSL Server (máy chủ) gồm các bước sau:

1. SSL Client gửi thông điệp “client hello” và thông tin mã hóa (Cryptographic information) đến SSL Server;
2. SSL Server gửi thông điệp “server hello”, các bộ mã hóa hỗ trợ (CipherSuite) và chứng chỉ máy chủ (Server certificate) đến SSL Client. SSL Server cũng có thể gửi yêu cầu máy khách cung cấp chứng chỉ máy khách (Client certificate) nếu cần thiết;
3. Nhận được yêu cầu, SSL Client kiểm tra chứng chỉ máy chủ và kiểm tra các tham số mã hóa. Hai bên thống nhất sử dụng các bộ mã hóa tốt nhất

| | | |
|---|--|-----------------|
|  | VIETTEL AI RACE | TD163 |
| | MỘT SỐ GIAO THỨC ĐẢM BẢO ATTT DỰA TRÊN MÃ HÓA | Lần ban hành: 1 |

cùng hỗ trợ cho phiên làm việc. Nếu chứng chỉ máy chủ không hợp lệ quá trình quá trình khởi tạo phiên kết thúc không thành công. Nếu chứng chỉ máy chủ hợp lệ tiếp tục bước tiếp theo;

4. Trao đổi khóa máy khách (Client key exchange). SSL Client sinh khóa phiên (hoặc các tham số mã hóa cho phiên), mã hóa khóa phiên sử dụng khóa công khai của SSL Server lấy từ chứng chỉ máy chủ và gửi cho SSL Server;
5. SSL Client cũng có thể gửi chứng chỉ máy khách cho máy chủ nếu được yêu cầu;
6. SSL Server sử dụng khóa riêng của mình để giải mã khôi phục khóa phiên gửi từ SSL Client. SSL Server cũng có thể kiểm tra chứng chỉ máy khách nếu cần thiết;
7. Client gửi thông điệp kết thúc khởi tạo phiên “Finished”;
8. Server gửi thông điệp kết thúc khởi tạo phiên “Finished”.

Sau khi quá trình khởi tạo thành công, hai bên SSL Client và SSL Server xác thực được các thông tin nhận dạng của nhau sử dụng chứng chỉ số, thông nhất các bộ mã hóa tốt nhất sử dụng và trao đổi được các khóa phiên, hoặc các tham số mã hóa phiên, hai bên thiết lập thành công kênh bảo mật cho truyền dữ liệu trong phiên.

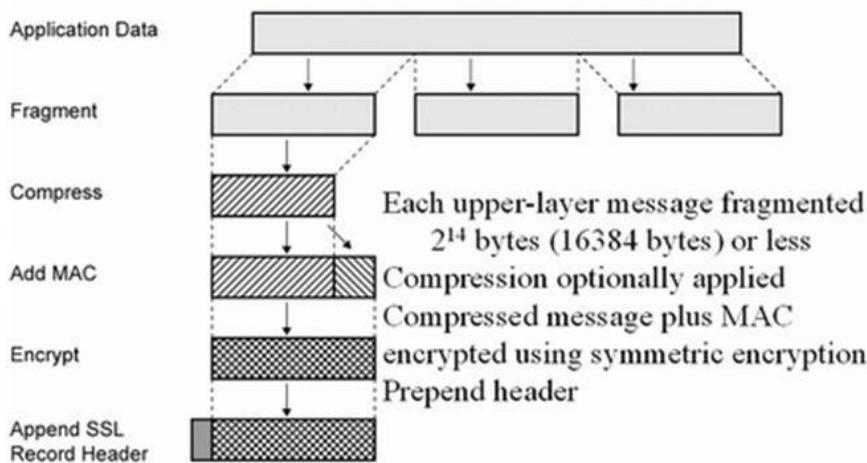
1.2.2 Vận chuyển dữ liệu an toàn

Quá trình vận chuyển dữ liệu an toàn thực hiện bởi giao thức SSL Record sau khi khởi tạo phiên làm việc thành công. Giao thức SSL Record sử dụng các tham số mã hóa và các bộ mã hóa thiết lập trong quá trình khởi tạo để tạo đường hầm vận chuyển dữ liệu an toàn. SSL Record đảm bảo tính bí mật cho khối dữ liệu sử dụng mã hóa đối xứng với khóa phiên, và đảm bảo tính toàn vẹn và xác thực cho khối dữ liệu sử dụng hàm băm có khóa (MAC). Hình 3.45 biểu diễn quá trình xử lý dữ liệu bởi SSL Record tại bên gửi, gồm các bước:

- Phân mảnh dữ liệu (Fragment): Dữ liệu từ ứng dụng (Application Data) được phân mảnh thành các khối cho phù hợp với việc đóng gói và truyền của các lớp giao thức tầng thấp hơn;

| | | |
|---|--|-----------------|
|  | VIETTEL AI RACE MỘT SỐ GIAO THỨC ĐẢM BẢO ATTT DỰA TRÊN MÃ HÓA | TD163 |
| | | Lần ban hành: 1 |

SSL Record Protocol Operation



Hình 3.45. Quá trình xử lý dữ liệu bởi SSL Record tại bên gửi

- Nén dữ liệu (Compress): Từng khối dữ liệu được nén để giảm kích thước.

Bước nén dữ liệu là không bắt buộc;

- Thêm MAC (Add MAC): Tính toán giá trị MAC (sử dụng hàm băm có khóa) cho khối dữ liệu nén và ghép giá trị MAC vào khối dữ liệu. Việc thêm MAC và kiểm tra MAC ở bên nhận để đảm bảo tính toàn vẹn và xác thực khối dữ liệu;
- Mã hóa (Encrypt): Mã hóa khối dữ liệu (gồm khối dữ liệu nén và MAC) để đảm bảo tính bí mật sử dụng mã hóa khóa đối xứng với khóa phiên;
- Thêm đè mục của SSL Record (Append SSL Record Header): thêm đè mục của SSL Record vào khối dữ liệu đã mã hóa và chuyển xuống tầng giao vận để chuyển sang bên nhận.

Quá trình xử lý dữ liệu khối dữ liệu nhận được tại bên nhận được thực hiện bởi SSL Record theo trình tự ngược lại, gồm các bước: Tách đè mục của SSL Record, Giải mã, Tách và kiểm tra MAC, Giải nén và Ghép các mảnh dữ liệu thành chuỗi dữ liệu để chuyển cho lớp ứng dụng.

2. SET

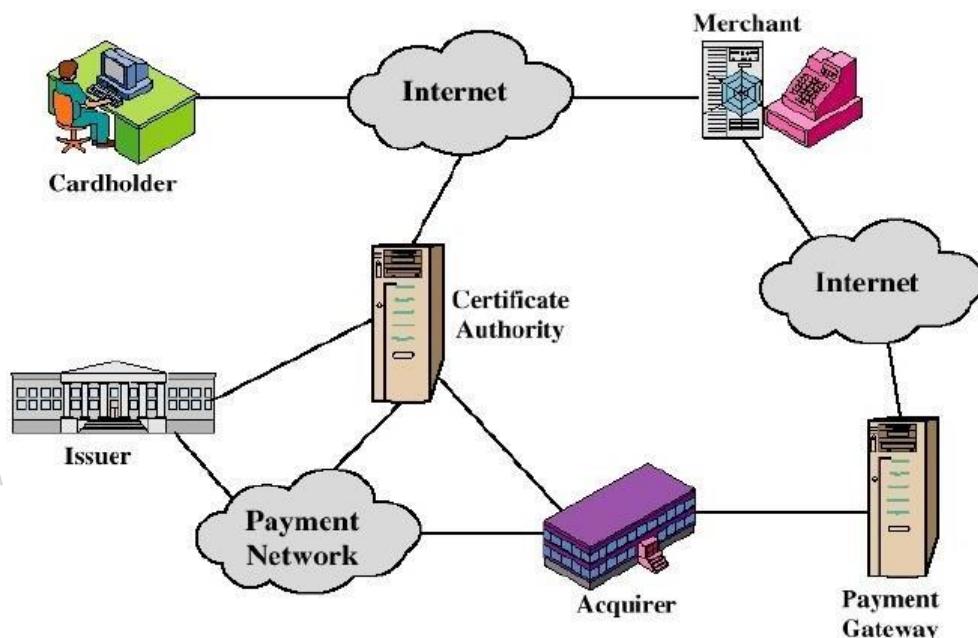
SET (Secure Electronic Transaction) là giao thức cho phép thanh toán điện tử an toàn sử dụng thẻ tín dụng do 2 công ty Visa International và MasterCard (Hoa Kỳ) phát triển. SET có khả năng đảm bảo các thuộc tính bí mật, toàn vẹn thông tin truyền, xác thực tài khoản chủ thẻ và xác thực nhà cung cấp.

Hình 3.46 biểu diễn một mô hình tương tác giữa các thực thể tham gia thực hiện SET. Các thực thể tham gia mô hình này gồm: Chủ thẻ/Khách hàng (Cardholder),

| | | |
|---|--|-----------------|
|  | VIETTEL AI RACE MỘT SỐ GIAO THÚC ĐẢM BẢO ATTT DỰA TRÊN MÃ HÓA | TD163 |
| | | Lần ban hành: 1 |

Nhà cung cấp dịch vụ/Người bán hàng (Merchant), Công thanh toán (Payment Gateway), Ngân hàng của nhà cung cấp/Ngân hàng của người bán (Acquirer), Ngân hàng của chủ thẻ/Ngân hàng của người mua (Issuer) và Nhà cung cấp chứng chỉ (Certificate Authority). Tất cả các bên tham gia quá trình xử lý giao dịch thanh toán (Cardholder, Merchant, Payment Gateway, Acquirer, Issuer) đều phải đăng ký với Nhà cung cấp

chứng chỉ và được cấp chứng chỉ khóa công khai. Các chứng chỉ khóa công khai được các bên sử dụng để xác thực thông tin nhận dạng của nhau và hỗ trợ trao đổi khóa. Quá trình thực hiện một giao dịch dựa trên SET gồm các bước sau:



Hình 3.46. Một mô hình tương tác giữa các thực thể tham gia SET

1. Khách hàng xem các sản phẩm trên website của Người bán hàng và quyết định các mặt hàng sẽ mua;
2. Khách hàng gửi thông điệp gồm thông tin đơn hàng và thanh toán gồm 2 phần: (i) Đơn hàng – dành cho Người bán hàng và (ii) Thông tin thẻ - dành cho hệ thống thanh toán;
3. Người bán hàng chuyển thông tin thẻ cho Công thanh toán. Công thanh toán chuyển tiếp cho Ngân hàng của người bán;
4. Ngân hàng của người bán gửi yêu cầu xác thực giao dịch thanh toán đến Ngân hàng của người mua;
5. Ngân hàng của người mua gửi xác nhận giao dịch đến Ngân hàng của người bán;
6. Ngân hàng của người bán gửi xác nhận giao dịch đến Người bán hàng;
7. Người bán hàng hoàn tất đơn hàng và gửi xác nhận đơn hàng đến Khách

| | | |
|---|--|-----------------|
|  | VIETTEL AI RACE MỘT SỐ GIAO THÚC ĐẢM BẢO ATTT DỰA TRÊN MÃ HÓA | TD163 |
| | | Lần ban hành: 1 |

hàng;

8. Người bán hàng ghi nhận giao dịch theo thông tin từ Ngân hàng người bán cung cấp;
9. Ngân hàng của người mua in hóa đơn giao dịch cho thẻ tín dụng của Khách hàng.

3. PGP

3.1 Giới thiệu

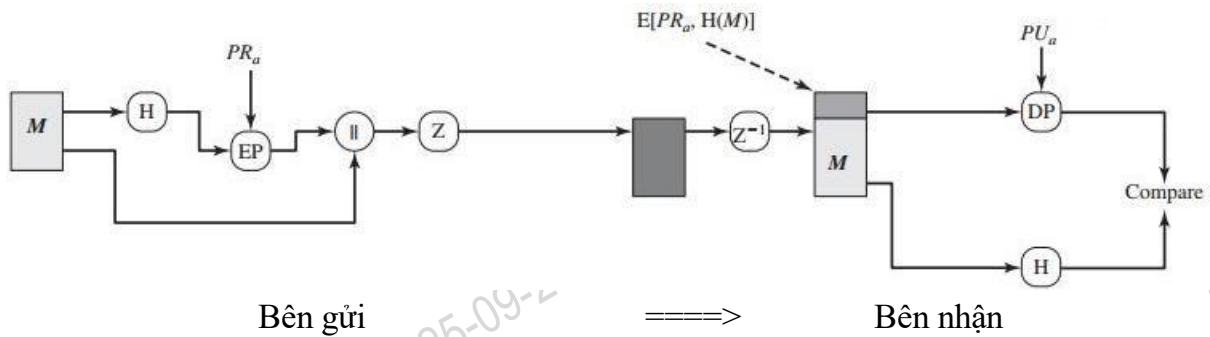
PGP (Pretty Good Privacy) là phương pháp bảo mật do Philip Zimmermann phát triển năm 1991 có khả năng cung cấp tính riêng tư và tính xác thực các thông điệp truyền. PGP được sử dụng rộng rãi và đã được thừa nhận thành chuẩn thực tế (RFC 3156). PGP hỗ trợ

mã hoá dữ liệu sử dụng mã hoá khoá bí mật và mã hóa khoá công khai, đồng thời cho phép tạo và kiểm tra chữ ký số.

PGP được sử dụng rộng rãi để truyền email và file an toàn. PGP hỗ trợ hầu hết các giải thuật mã hóa hiện đại như 3DES, AES, IDEA, RSA, ElGamal. Có nhiều bản cài đặt PGP trên thực tế như OpenPGP, GnuPG, Gpg4win,....

3.2 Hoạt động của PGP

PGP hỗ trợ 3 mô hình hoạt động, bao gồm (1) Mô hình PGP chỉ đảm bảo tính xác thực thông điệp, (2) Mô hình PGP chỉ đảm bảo tính bí mật thông điệp và (3) Mô hình PGP đảm bảo tính bí mật và xác thực thông điệp. Để thuận tiện cho mô tả hoạt động của các mô hình PGP, gọi H là hàm băm một chiều, EC là hàm mã hóa khóa đối xứng, DC là hàm giải mã khóa đối xứng, EP là hàm mã hóa khóa bất đối xứng, DP là hàm giải mã khóa bất đối xứng, Z là hàm nén, Z^{-1} là hàm giải nén, PUa là khóa công khai của bên A, PRa là khóa riêng của bên A, PUB là khóa công khai của bên B, PRb là khóa riêng của bên B và Ks là khóa phiên. Phần tiếp theo trình bày chi tiết về hoạt động của các mô hình này.



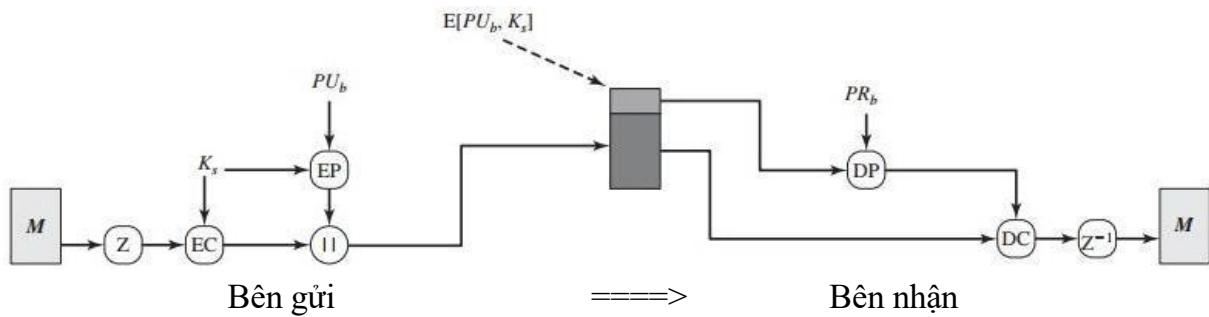
Hình 3.47. Mô hình PGP chỉ đảm bảo tính xác thực thông điệp

Hình 3.47 biểu diễn mô hình PGP chỉ đảm bảo tính xác thực thông điệp truyền.

| | | |
|---|--|-----------------|
|  | VIETTEL AI RACE MỘT SỐ GIAO THÚC ĐẢM BẢO ATTT DỰA TRÊN MÃ HÓA | TD163 |
| | | Lần ban hành: 1 |

Theo đó, mô hình này sử dụng chữ ký số để xác thực tính toàn vẹn và chủ thể gửi thông điệp. Điều kiện thực hiện mô hình này là bên gửi A phải sở hữu cặp khóa (khóa công khai PUa và khóa riêng PRa). Quá trình thực hiện gửi/nhận thông điệp M đảm bảo tính xác thực tại mỗi bên như sau:

- Bên gửi A:
 - + Tính toán giá trị băm (giá trị đại diện) của thông điệp M sử dụng hàm băm H;
 - + Sử dụng khóa riêng PRa để mã hóa (ký) giá trị băm của M tạo thành chữ ký số;
 - + Ghép chữ ký số vào thông điệp M ;
 - + Nén thông điệp và chữ ký số sử dụng hàm nén Z;
 - + Gửi bản dữ liệu đã nén cho người nhận.
- Bên nhận B:
 - + Giải nén dữ liệu nhận được sử dụng hàm Z^{-1} ;
 - + Tách chữ ký số khỏi thông điệp M và sử dụng khóa công khai của bên gửi PUa để kiểm tra (giải mã) chữ ký số để khôi phục giá trị băm h1. Bên gửi A có thể sử dụng các phương pháp trao đổi khóa công khai đã nêu ở mục 3.5.3 để chuyển khóa công khai PUa cho bên nhận;
 - + Tính toán giá trị băm h2 của thông điệp M sử dụng hàm băm H;
 - + So sánh 2 giá trị băm h1 và h2, nếu $h1 = h2$ thì thông điệp truyền là toàn vẹn và thông điệp được gửi bởi bên gửi A. Nếu $h1 \neq h2$ thì thông điệp M có thể đã bị sửa đổi, hoặc không được ký và gửi bởi bên gửi A.



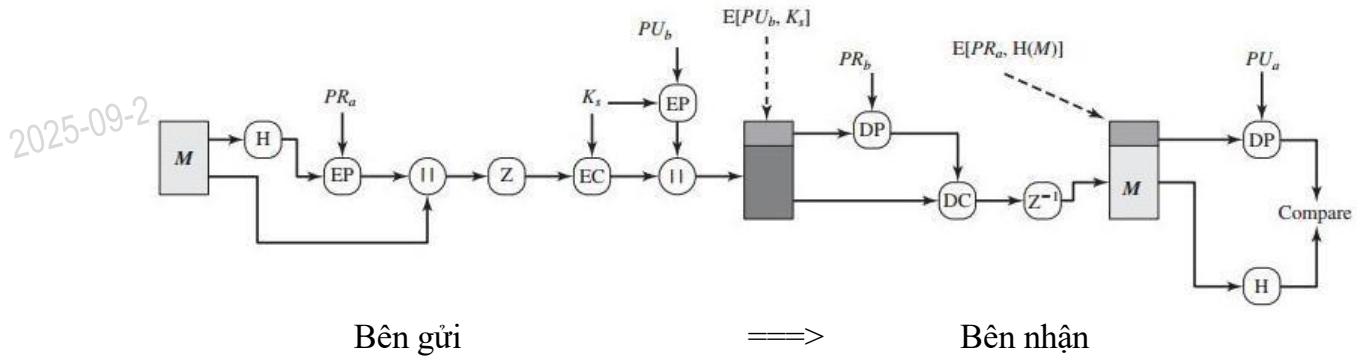
Hình 3.48. Mô hình PGP chỉ đảm bảo tính bí mật thông điệp

Hình 3.48 biểu diễn mô hình PGP chỉ đảm bảo tính bí mật thông điệp truyền. Theo đó, mô hình này sử dụng kết hợp giữa mã hóa khóa đối xứng và mã hóa khóa bất đối xứng để đảm bảo tính bí mật của thông điệp. Điều kiện thực hiện mô hình này là bên nhận B phải sở hữu cặp khóa (khóa công khai PUb và khóa riêng PRb). Quá trình thực hiện gửi/nhận thông điệp M đảm bảo tính bí mật tại mỗi bên như sau:

- Bên gửi A:

| | | |
|---|--|-----------------|
|  | VIETTEL AI RACE MỘT SỐ GIAO THỨC ĐẢM BẢO ATTT DỰA TRÊN MÃ HÓA | TD163 |
| | | Lần ban hành: 1 |

- + Nén thông điệp M sử dụng hàm nén Z ;
 - + Sinh khóa phiên K_s và sử dụng khóa K_s để mã hóa thông điệp M sử dụng hàm mã hóa đối xứng EC ;
 - + Sử dụng khóa công khai PU_b của bên nhận B để mã hóa khóa phiên K_s sử dụng hàm mã hóa bất đối xứng EP . Bên nhận B có thể sử dụng các phương pháp trao đổi khóa công khai đã nêu ở mục 3.5.3 để chuyển khóa công khai PU_b cho bên gửi;
 - + Ghép chữ bản mã của K_s vào bản mã của thông điệp M ;
 - + Gửi bản mã dữ liệu cho người nhận.
- Bên nhận B :
- + Tách bản mã của K_s vào bản mã của thông điệp M ;
 - + Giải mã bản mã K_s sử dụng hàm giải mã khóa bất đối xứng DP và khóa riêng PR_b để khôi phục K_s ;
 - + Sử dụng khóa phiên K_s và hàm giải mã khóa đối xứng DC để giải mã khôi phục thông điệp đã nén M ;
 - + Giải nén khôi phục thông điệp M sử dụng hàm Z^{-1} ;



Hình 3.49. Mô hình PGP đảm bảo tính bí mật và xác thực thông điệp

Hình 3.49 biểu diễn mô hình PGP đảm bảo tính xác thực và bí mật thông điệp truyền. Theo đó, mô hình này sử dụng chữ ký số để xác thực tính toàn vẹn và chủ thể gửi thông điệp. Đồng thời mô hình sử dụng kết hợp giữa mã hóa khóa đối xứng và mã hóa khóa bất đối xứng để đảm bảo tính bí mật của thông điệp. Điều kiện thực hiện mô hình này là bên gửi A phải sở hữu cặp khóa (khóa công khai PUa và khóa riêng PRa) và bên nhận B phải sở hữu cặp khóa (khóa công khai PUb và khóa riêng PRb). Mô hình này là sự kết hợp của mô hình PGP chỉ đảm bảo tính xác thực và mô hình PGP chỉ đảm bảo tính bí mật. Theo đó, bên gửi A thực hiện ký và mã hóa thông điệp, còn bên nhận B thực hiện giải mã và kiểm tra chữ ký của thông điệp.