

Thuyết h 2.

Câu 1. cho $p = 7$, $q = 11$, $e = 17$

- Thực hiện phát sinh khóa công khai và khóa riêng theo RSA

$$p = 7, q = 11 \rightarrow n = p \cdot q = 77$$

$$\phi(n) = (p-1)(q-1) = 60$$

cho $e = 17$, tìm $d = e^{-1} \bmod \phi(n) = 53$

Áp dụng thuật toán Euclid mở rộng.

$q = r_{i-1} / r_i$	$r_{i-1} = \phi(n)$	$r_i = e$	$r = r_{i-1} - q \cdot r_i$	t_1	t_2	$t = t_1 - q \cdot t_2$
3	60	17	$60 - 3 \cdot 17 = 9$	0	1	$0 - 3 \cdot 1 = -3$
1	17	9	$17 - 1 \cdot 9 = 8$	1	-3	$1 - 1 \cdot (-3) = 4$
1	9	8	$9 - 1 \cdot 8 = 1$	-3	4	$-3 - 1 \cdot 4 = -7$
8	8	1	$8 - 1 \cdot 8 = 0$	4	-7	$4 - 8 \cdot (-7) = 60$
	1	0		-7	60	

Vì $t_1 = -7 < 0$ nên $d = t_1 + \phi(n) = -7 + 60 = 53$

Vậy khóa công khai: $\{e, n\} = \{17, 77\}$

khóa riêng: $\{d, n\} = \{53, 77\}$.

- Tạo ra hàm mã chữ ký RSA (mã hóa chứng thư)

Cho thông điệp $M = 9$

$M = 9$, $PU = \{17, 77\}$, $PR = \{53, 77\}$

Mã hóa bằng thao tác như sau:

$$C \equiv M^e \pmod{n} = 9^{17} \pmod{77}$$

Áp dụng thuật toán bình phương nhanh

Số mũ	C	d
$17_{(10)} = 10001_{(2)}$	0	1
1	1	$(d \times d \times a) \pmod{n} = 9$
0	2	$d \times d \pmod{n} = 4$
0	4	$d \times d \pmod{n} = 16$
0	8	$d \times d \pmod{n} = 25$
1	17	$d \times d \times a \pmod{n} = 4$

Vậy $C = 4$

$C = 4$, Mod 103, 77.

Giải mã $M = C^d \mod n = 4^{53} \mod 77$.

Số mũ	C	d
$53_{(10)} = \underline{110101}_{(2)}$	0	1
1	1	$d \times d \times a \mod n = 4$
1	3	$d \times d \times a \mod n = 64$
0	6	$d \times d \mod n = 16$
1	13	$d \times d \times a \mod n = 53$
0	26	$d \times d \mod n = 37$
1	53	$d \times d \times a \mod n = 9$

Câu 2. SSL là gì? tại sao cần SSL? Dân hiện nhận biết? Cách hoạt động

SSL (Secure Sockets Layer) là một công nghệ mã hóa thông tin giữa máy khách và máy chủ trên internet, giúp bảo vệ dữ liệu khi chúng được truyền qua mạng. SSL thường được sử dụng để bảo vệ thông tin nhạy cảm như thông tin cá nhân, thông tin tài khoản ngân hàng, mật khẩu và các dữ liệu khác tương tự.

Lớp công nghệ mạng (SSL) cung cấp dịch vụ bảo mật giữa TCP và các ứng dụng sử dụng TCP. Chuẩn internet cơ bản là

Transport Layer Service (TLS). SSL/TLS cung cấp hình thức mã hóa cách sử dụng mã hóa để xác minh tính toàn vẹn và tin cậy bằng mã xác thực tin nhắn.

SSL/TLS bao gồm các cơ chế giao thức cho phép hai người dùng TCP xác định các cơ chế và dịch vụ bảo mật mã hóa sử dụng.

- HTTPS (http qua ssl) để cấp được kết nối giữa HTTP và ssl để thực hiện giao tiếp an toàn giữa trình duyệt web và máy chủ web.

- Secure shell (SSH) cung cấp khả năng truy cập từ xa an toàn và các cơ sở máy khách / máy chủ an toàn khác.

* Tại sao cần cài SSL?

Việc cài đặt SSL là cần thiết vì nó giúp tăng cường bảo mật mạng cho dữ liệu truyền qua mạng. SSL giúp ngăn chặn tin tặc, kẻ tấn công mạng nghe lén, sửa đổi thay đổi nội dung, cấp quyền truy cập máy chủ, thay đổi cấu hình mạng, thay đổi dữ liệu khách hàng, giả mạo dữ liệu. Ngoài ra, còn giúp xác nhận rằng bạn đang kết nối với trang web chứ không phải là kẻ lừa đảo.

* Dẫn hướng nhận biết?

1. URL của trang web bắt đầu bằng "https://" thay vì "http://". Chữ "s" ở đây đại diện cho "secure" (an toàn).

2. Xuất hiện từ ô hoạt hoặc biên tập báo mới ở
thời điểm cơ thể dưới

3. Có thể nào cải tạo ở thời điểm xem "Chứng chỉ hợp lệ"

* Cách thức hoạt động của SSL

1. Máy chủ gửi yêu cầu kết nối an toàn tới máy chủ

2. Máy chủ gửi chứng chỉ SSL (chứa gồm thông tin về máy chủ và
chìa khóa công khai)

3. Máy khách xác nhận chứng chỉ SSL và tạo mã khóa phiên mã
hóa mới.

4. Máy khách gửi khóa phiên mã mã hóa tới máy chủ

5. Máy chủ gửi mã khóa phiên mã xác nhận

6. Quá trình trao đổi dữ liệu giữa máy khách và máy chủ tiếp
tục với khóa phiên mã tạo.

Câu 3. Tình huống.

- Các chức năng như: tìm kiếm các loại sách, đây là một
sách hoặc từ khóa tìm kiếm sách sẵn dùng:

④ Nếu như nơi đi tìm sách sẵn dùng thì việc tìm kiếm 1 cuốn
sách là rất khó, việc đây hệ thống sách gây khó khăn cho
sinh viên hoặc việc từ từ tìm kiếm. Việc mất đi một số
chức năng sinh viên, người dùng thay thế truy cập.

- Việc đặt mua, thanh toán phí mua trực tuyến ngay trên trang web cần được nâng cao hơn nữa.

① Cần nâng cao bậc nữa, trước nữa là mặt thấy tin, mặt tiền hay tài khoản. Trang lúc giao dịch có thể bị hacker tấn công truy cập vào thay đổi hoặc chuyển tiền của sinh viên đi mất thay vì được thanh toán cho chính các giao dịch sách trên trang web. Gây ra mất tiền bạc, lợi ích của sinh viên, ảnh hưởng danh tiếng của trang web. Hệ thống cũng như chập chờn.

b) Đưa ra giải pháp để cải thiện hệ thống cao tính an toàn

- Đối với hệ thống chức năng: ta sẽ dùng cho phép truy cập tài khoản mật khẩu do hệ thống cấp cho sinh viên, giáo viên, người dùng (mật khẩu fixed password).

=> Xác thực bằng tài khoản mật khẩu, tài khoản đến lại từ xác thực cho tài khoản, tránh được việc giả mạo, tấn công dịch vụ DDOS gây tắc nghẽn hệ thống nhân viên đảm bảo thời gian dùng các chức năng.

- Đối với Thanh toán trực tuyến: ta sẽ dùng kết hợp tài khoản ngân hàng với SMS OTP đến số điện thoại của người dùng nhằm chứng thực giao dịch. Mỗi lần giao dịch hệ thống

Sẽ gửi câu nháy mật mã OTP ~~nhắn~~ cho thuê gửi qua SMS.
⇒ Vì OTP là mã chỉ 1 lần sử dụng nó có hiệu lực trong
khoảng thời gian nhất định, thời gian ngắn nên thuê lợi từ số dư
cấp hoặc lần gửi. Tin nhắn SMS OTP sẽ được gửi đến 30T
người dùng, điều đó xảy ra bất ngờ cho thuê từ nhà hàng.
Thành  mặt cười.