Bài tập 15: Chữ ký số

Câu hỏi 1

Chính phủ muốn tạo ra một kênh tư vấn cho công chúng đảm bảo rằng không ai có thể giả mạo tin nhắn hoặc khuyến nghị từ chính phủ. Phương pháp mật mã nào dưới đây hiệu quả nhất để giải quyết vấn đề này?

1. Dùng nhiều mã xác thực thông điệp, mỗi người dân sẽ có một khoá duy nhất, và sinh tag cho mỗi người mỗi khi chính phủ đưa ra khuyến nghị.
2. Dùng một hệ mật mã khoá công khai, với khoá công khai mọi người đều biết, và giải mã mỗi khuyến nghị được đưa ra.
3. Dùng sơ đồ chữ ký số, với khoá công khai mọi người đều biết, để ký mỗi khuyến nghị được đưa ra.
4. Dùng mã xác thực, với khoá mọi người đều biết, để sinh một tag cho mỗi khuyến nghị được đưa ra.

Câu hỏi 2

Ngài chủ tịch và phó chủ tịch của một công ty muốn trao đổi thông tin với nhau theo cách đảm bảo tính toàn vẹn thông tin. Phương pháp mật mã nào dưới đây hiệu quả nhất để giải quyết vấn đề này?

1. Dùng mã xác thực thông điệp, với khoá chia sẻ hai bên, và sinh tag cho mỗi thông điệp họ gửi.
2. Dùng mã xác thực thông điệp, với khoá mọi người đều biết, và sinh tag cho mỗi thông điệp họ gửi.
3. Dùng sơ đồ chữ ký số, với khoá công khai mọi người đều biết, và ký mỗi thông điệp họ gửi.
4. Dùng một hệ mã hoá khoá đối xứng, với khoá chia sẻ giữa họ, và mã hoá mỗi thông điệp họ gửi.

Câu hỏi 3

Giả sử (cho câu hỏi này) rằng sơ đồ chữ ký số chỉ ký thông điệp 256-bit và có thời gian ký chậm hơn 100 lần so với việc tính SHA-256 trên dữ liệu 512-bit. Đáp án nào dưới đây là đúng nếu ta muốn ký thông điệp M kích thước $500MB$?

1. Ký M dùng sơ đồ đưa ra là không thể, vì nó chỉ cho phép ký thông điệp 256-bit.
2. Ta có thể ký M đơn giản bằng cách băm nó, và tránh kết hợp với sơ đồ chữ ký số.

3. Ta có thể ký an toàn M bằng cách tách nó thành các khối 256-bit, và ký lên từng khối.
4. Nếu sơ đồ băm-và-ký được dùng, thì việc ký M sẽ mất thời gian xấp xỉ bằng với thời gian băm M.

Câu hỏi 4

Xét sơ đồ chữ ký RSA "đơn giản" với khoá công khai $(N = 55, e = 3)$. Giá trị nào dưới đây là chữ ký hợp lệ cua thông điệp $m = 17$?

1. 7
2. 4
3. $8^3 = 17 \bmod 55$
4. 43

Câu hỏi 5

Xét sơ đồ chữ ký RSA "đơn giản" với khoá công khai $(N, e = 3)$. Đối với những thông điệp nào sau đây, ta luôn luôn có thể giả mạo chữ ký dù không thấy bất kỳ chữ ký nào trước đó và không có phân tích thừa số của N? (Giả sử $N > 1000$ và N nguyên tố cùng nhau với mỗi thông điệp dưới đây.)

1. 2
2. 27 $= 3^3 = 27 \bmod N$
3. 47
4. 37

Câu hỏi 6

Xét sơ đồ chữ ký RSA "đơn giản" với khoá công khai (N, e). Giả sử ta muốn giả mạo chữ ký của $m = 289$ nhưng ta chỉ có được chữ ký của một thông điệp khác. Chiến lược nào dưới đây sẽ hiệu quả? (Giả sử $N > 1000$.)

1. Lấy được chữ ký σ trên $m' = 288$. Đưa ra $[\sigma + 1 \mod N]$ làm chữ ký của m.
2. Lấy được chữ ký σ trên $m' = 17$. Đưa ra $[\sigma^2 \mod N]$ làm chữ ký của m. $17^2 = 289$
3. Lấy được chữ ký σ trên $m' = 578$. Đưa ra $[2^{-1} \cdot \sigma \mod N]$ làm chữ ký của m.
4. Lấy được chữ ký σ trên $m' = 288$. Đưa ra $[\sigma - 1 \mod N]$ làm chữ ký của m.

Câu hỏi 7

Cho sơ đồ chữ ký RSA với khoá công khai $(n = 9797, e = 131)$, chữ ký nào dưới đây là hợp lệ?

- $(m = 123, \sigma = 6292)$
- $(m = 4333, \sigma = 4768)$

- $(m = 4333, \sigma = 1424)$

Câu hỏi 8

Cho sơ đồ chữ ký RSA với khoá công khai $(n = 9797, e = 131)$, chỉ ra cách Oscar có thể tấn công giả mạo chữ ký bằng cách đưa ra một ví dụ tấn công cho tham số RSA này.

Câu hỏi 9

Ta xem xét sơ đồ chữ ký ElGamal. Bạn có khoá bí mật của Bob $sk = d = (67)$ và khoá công khai tương ứng $pk = (p, g, g^d) = (97, 23, 15)$.

1. Hãy tính chữ ký Elgammal (r, s) và kiểm tra thông điệp từ Bob gửi Alice cho thông điệp m và khoá tạm thời k_E dưới đây:
   (a) $m = 17$ và $k_E = 31$
   (b) $m = 17$ và $k_E = 49$
   (c) $m = 85$ và $k_E = 77$
2. Bạn nhận được hai thông điệp m_1, m_2 và chữ ký tương ứng (r_i, s_i) được cho là từ Bob. Hãy kiểm tra liệu các

$$(m_1, r_1, s_1) = (22, 37, 33) \quad \text{và} \quad (m_2, r_2, s_2) = (82, 13, 65)$$

   có phải được gửi từ Bob không?

Câu hỏi 10

Cho hệ chữ ký Elgamal với $p = 31, g = 3$ và $pk = g^d = 6$. Bạn nhận được thông điệp $m = 10$ hai lần với hai chữ ký (r, s) khác nhau:

$$(17, 5) \quad \text{và} \quad (13, 15)$$

1. Liệu có phải cả hai chữ ký đều hợp lệ?
2. Có bao nhiêu chữ ký hợp lệ cho mỗi thông điệp m và với tham số xác định ở trên?

Câu hỏi 11

Cho sơ đồ chữ ký Elgamal với khoá công khai $pk = (p = 97, g = 23, g^d = 15)$. Chứng minh rằng Oscar có thể thực hiện tấn công giả mạo thông điệp bằng cách đưa ra một ví dụ cho một chữ ký hợp lệ.

Câu hỏi 12

Cho sơ đồ chữ ký Elgamal với tham số công khai $p, g \in \mathbb{Z}_p^*$ và khoá bí mật $sk = d$. Do cài đặt sai, hệ gây ra sự phụ thuộc giữa hai khoá tạm thời liền nhau

$$k_{E_{i+1}} = k_{E_i} + 1$$

Hơn nữa, hai chữ ký liền nhau của bản rõ m_1 và m_2 được đưa ra

$$(r_1, s_1) \qquad \text{và} \qquad (r_2, s_2)$$

Hãy giải thích cách mà kẻ tấn công có thể tính khoá bí mật với các giá trị đưa ra.

Câu hỏi 13

Tham số của DSA được cho bởi $p = 59, q = 29, g = 3$, và khoá bí mật của Bob là $sk = d = 23$. Chỉ ra quá trình ký (Bob) và kiểm tra chữ ký (Alice) cho các mã băm $h(m)$ và khoá tạm thời k_E sau đây:

1. $h(m) = 17,\ k_E = 25$
2. $h(m) = 2,\ k_E = 13$
3. $h(m = 21,\ k_E = 8)$

Câu hỏi 14

Chỉ ra cách tấn công DSA nếu cùng một khoá tạm thời lại được dùng để ký hai thông điệp khác nhau.