Started on	Sunday, 12 March 2023, 9:33 PM
State	Finished
Completed on	Sunday, 12 March 2023, 9:45 PM
Time taken	12 mins 26 secs

Question **1**

Complete

Marked out of 1.00

Hãy tìm mệnh đề đúng nhất dưới đây

Người ta giả mạo văn bản có chữ ký điện tử thông qua một quá trình:

a. Tìm hai văn bản có cùng giá trị băm và có nội dung cùng chủ đề nhưng khác biệt trên một vài yếu tố quan trọng

b. Tìm hai văn bản có nội dung khác nhau mà có giá trị băm giống nhau

c. Người ta xây dựng 2 tập văn bản có nội dung là đối lập nhau theo 1 nghĩa nào đó và đồng thời băm rồi tìm 2 văn bản có cùng giá trị băm

d. Xuất phát từ một văn bản gốc, tìm cách thêm/bớt các dấu trắng ở rất nhiều vị trí để sinh ra nhiều văn bản, từ đó tìm được 2 văn bản có cùng giá trị băm

Question **2**

Complete

Marked out of 1.00

Hãy chỉ ra phát biểu đúng dưới đây

- a. Φ(15) = 8 và Φ(101)= 100
- b. Φ(p*q*r) = (p-1)(q-2)(r-3) nếu p, q và r đều là số nguyên tố
- c. Φ(105)=48 và Φ(21)=16
- d. Φ(21)= 12 và Φ(12)=11

Question **3**

Complete

Marked out of 1.00

Theo giải thuật tính lũy thừa nhanh, tính X^a mod n sẽ cần khoảng bao nhiêu phép bình phương đồng dư khi a có giá trị cỡ 1 tỷ

- a. 10 lần
- b. 50 lần
- c. 40 lần
- d. 20 lần
- e. 30 lần

Question **4**

Complete

Marked out of 1.00

Trong hệ RSA với e=11, p=11 và q =13 thì bản rõ 3 bit X=101 sẽ có bản mã tương ứng là gì?

a. 111100

b. 110100

c. 100100

d. 101101

e. 110111

Question **5**

Complete

Marked out of 1.00

Nếu A muốn gửi một văn bản X cho B sao cho vừa bảo mật vừa đảm bảo xác thực thì có thể thực hiện mã hóa trước khi gửi theo cách nào? Lưu ý ZA và zA là khóa công khai và bí mật của A, ZB và zB là khóa công khai và bí mật của B.

a. $E_{ZA}\ (D_{zB}\ (X))$

b. $E_{ZB}\ (D_{zA}\ (X))$

c. $D_{zB}\ (E_{ZA}\ (X))$

d. $D_{zA}\ (E_{ZB}\ (X))$

Question **6**

Complete

Marked out of 2.00

Khi tạo mã Vigenere với cùng một bản rõ, sử dụng khóa nào sẽ tạo ra bản mã có hệ số trùng khớp (IC) lớn nhất:

a. "Lovely"

b. "abcdef"

c. “aaaaaaaaabbbbbbccccc”

d. “Mississippii”

e. "HelloBill"

Question **7**

Complete

Marked out of 3.00

Gọi X là giá trị tạo bởi 2 chữ số cuối của MSSV của em, gọi Y là giá trị tính được qua MSSV (của em) mod 4; ví dụ với MSSV đuôi 93 sẽ có X=93, Y=1.

Giả sử **H** là một hàm băm với kích thước đầu ra là (Y+2)*16 bits. Giả sử Scorp-***i*** (***i***=1-9) là một con chip có khả năng thực hiện 10^{i} *100 phép băm **H** trong một giây (ví dụ, Scorp-2 có thể thực hiện 10000 phép băm trong một giây). Đây là con chip có tốc độ nhanh nhất và kinh tế nhất trong cùng loại trên thị trường với đơn giá $i^{i/2}$ *$1000 (VD: Scorp-2 có giá $2000, Scorp-4 có giá $16000).

Một hệ thống xác thực yêu cầu người dùng chọn mật khẩu có 6 ký tự trên bảng chữ kích thước N=(X mod 50)+ 50.

Hãy xét một giao thức xác thực mật khẩu gồm 3 bước như sau: 1) Alice yêu cầu đăng nhập; 2) Hệ thống gửi Alice một giá trị ngẫu nhiên R; 3) Alice đáp ứng bằng việc gửi trả $H(H(Password_A)||R)$ trong đó || ký hiệu phép ghép nối xâu. Hệ thống cho phép nhiều lần thử đăng nhập liên tục nhưng không quá 10 phút kéo dài tổng cộng nếu chưa thành công (hết 10 phút sẽ cắt đường truyền và treo tài khoản). Một kẻ tấn công muốn đột nhập tài khoản của Alice bằng cách thử đăng nhập từ xa liên tục, nếu kẻ tấn công sử dụng một chip Scorp-2 thì cơ hội thành công sẽ như thế nào?

Để tính toán cơ hội thành công của kẻ tấn công, chúng ta cần tính toán số lượng phép băm tối đa mà kẻ tấn công có thể thực hiện trong 10 phút. Đầu tiên, ta tính kích thước của đầu vào cho hàm băm H:

Y + 2 = 2

Kích thước đầu vào cho H là 2 * 16 bits = 32 bits.

Tiếp theo, ta tính kích thước của mật khẩu:

N = (X mod 50) + 50 = 72 mod 50 + 50 = 72

Mật khẩu có 6 ký tự, do đó mỗi ký tự sẽ có log_2{72} bits. Vậy độ dài của mật khẩu là 6 x log_2{72} bits.

Chúng ta sử dụng phương pháp băm theo thời gian, giả sử thời gian băm 1 lần là 1/10000 giây. Khi đó, số lượng phép băm tối đa mà kẻ tấn công có thể thực hiện trong 10 phút là:

10 x 60 x 10000 = 6 x 10^6 phép băm.

Cơ hội thành công của kẻ tấn công phụ thuộc vào số lần thử đăng nhập tối đa mà họ có thể thực hiện trong số lượng phép băm tối đa trên. Để tính toán số lần thử đăng nhập tối đa, chúng ta cần tính số lượng giá trị ngẫu nhiên R có thể có. Vì độ dài của R là 2xlog_2{72} bits, số lượng giá trị ngẫu nhiên có thể có là 2^{2log_2{72}} = 72^2 = 5184

Số lần thử đăng nhập tối đa mà kẻ tấn công có thể thực hiện là:

6 x 10^6 / 5184 =1158

Vậy cơ hội thành công của kẻ tấn công là khoảng 1/1158. Tuy nhiên, nếu kẻ tấn công sử dụng một chip Scorp-2, thì số lượng phép băm tối đa mà họ có thể thực hiện trong 10 phút là $10^4 \times 10^2 \times 2 = 2 \times 10^7$, gấp đôi so với trường hợp không có chip Scorp-2. Do đó, cơ hội thành công của kẻ tấn công sẽ tăng lên gấp đôi, khoảng 1/579.

◄ Announcements

Jump to...