Quiz 8 - Hàm băm và HMAC

Tổng điểm 8/8

Các câu hỏi lựa chọn có thể có nhiều hơn 1 đáp án. Cần phải lựa chọn tất cả đáp án đúng.

MSSV *

20200497

Câu 1. Giả sử H(m) là một hàm băm mật mã an toàn. Người ta muốn tạo ra một hàm băm mới H'(x). Cách thiết kế hàm băm nào sau đây thỏa mãn là hàm 1 chiều?(Chọn tất cả đáp án đúng) 1/1

- [x] H'(m) = H(m) mod 100
- [x] H'(m) = pow(g, m) mod p, trong đó pow() là hàm lũy thừa, p là số nguyên tố và g là giá trị ngẫu nhiên
- [ ] H'(m) = m*m;
- [x] H'(m) = H(m) || "end"
- [x] H'(m) = H(H(m))
- [x] H'(m) = 1/2 số bit đầu tiên của m

Câu 2. Giả sử H(m) là một hàm băm mật mã an toàn. Người ta muốn tạo ra một hàm băm mới H'(x). Cách thiết kế hàm băm nào sau đây có khả năng chống đụng độ?(Chọn tất cả đáp án đúng) 1/1

- [x] H'(m) = H(H(m))
- [ ] H'(m) = m*m;
- [ ] H'(m) = 1/2 số bit đầu tiên của m
- [x] H'(m) = H(m) || "end"
- [ ] H'(m) = H(m) mod 100
- [ ] H'(m) = pow(g, m) mod p, trong đó pow() là hàm lũy thừa, p là số nguyên tố và g là giá trị ngẫu nhiên

Câu 3. Giả sử Alice và Bob đã chia sẻ một khóa bí mật k. Alice gửi cho Bob bản tin E(k, m) || H(E(k, m)), trong đó E là mã hóa AES-CBC còn H là hàm băm mật mã an toàn. Sơ đồ này thỏa mãn yêu cầu nào? 1/1

- [x] Tính bí mật (Confidentiality)
- [ ] Tính xác thực toàn vẹn (Integrity)
- [ ] Tính xác thực danh tính (Authenticity)
- [ ] Không thỏa mãn yêu cầu nào

Câu 4. Giả sử Alice và Bob đã chia sẻ một khóa bí mật k. Alice gửi cho Bob bản tin E(k, m) || H(k || E(k, m)), trong đó E là mã hóa AES-CBC còn H là hàm băm SHA-1. Sơ đồ này thỏa mãn yêu cầu nào? 1/1

- [x] Tính bí mật (Confidentiality)
- [ ] Tính xác thực toàn vẹn (Integrity)
- [ ] Tính xác thực danh tính (Authenticity)
- [ ] Tất cả các yêu cầu

Câu 5. Một hàm băm mật mã an toàn có kích thước đầu ra là 50 bit. Chọn trước 1 giá trị băm là x thì xác suất xuất hiện của bản tin m có H(m) = x là bao nhiêu? 1/1

- ( ) 0.02
- ( ) 1/2^25
- (•) 1/2^50

Câu 6. Một hàm băm mật mã an toàn có kích thước đầu ra là 60 bit. Nếu chúng ta có hệ thống máy tính có khả năng thực hiện hàm băm trong 1 ns (nanosecond) thì mất bao nhiêu năm để tìm ra được bản tin m sao cho H(m) = x với x chọn trước?(Ghi đáp án là phần nguyên) 1/1

36

Câu 7. Khi tấn công dựa trên nghịch lý ngày sinh vào hàm băm SHA-1 để tìm ra các bản tin đụng độ, theo kỳ vọng thì số lượng bản tin phải kiểm tra sẽ giảm đi bao nhiêu lần? 1/1

- 2
- 80
- 2^40
- 2^79
- 2^80

Câu 8. Một sơ đồ mật mã sử dụng chế độ CBC với khóa k = (k1, k2). Trong đó, k1 được sử dụng để tạo giá trị IV = HMAC(k1, m) còn k2 được sử dụng để mã hóa bản tin E(k2, m). Nếu khóa k được dùng nhiều lần, phát biểu nào sau đây là đúng? 1/1

- ○ Sơ đồ này không chống được tấn công CCA nhưng chống được tấn công CPA
- ◉ Sơ đồ này không chống được tấn công CPA
- ○ Sơ đồ này không chống được tấn công KPA
- ○ Sơ đồ này chống được tấn công CCA