ĐÁP ÁN VẮN TẮT CHO ĐỀ THI NMATTT 2021.2

Để tránh sự học theo lối "học gạo" kiểu ôn và sao chép lời giải đề cũ, thầy không đưa đáp án đầy đủ.

1. Hai chế độ mật mã nào có khả năng đáp ứng tính toán song song: **(2pt)**
   a) CBC và CTR; b) ECB và OFG; c) CBC và CTR; d) ECB và CTR;

Đáp án: d

2. Từ cùng một bản rõ, hệ số trùng khớp (IC) tính theo khóa nào sẽ là lớn nhất: **(3pt)**
   a) "HelloBill" b)"Lovely" c) "abcdef" d) "Mississippii" e) "aaaaaaaaabbbbbbccccc"

Đáp án: e, số bảng thế thực chất chỉ là 3 – nhỏ nhất có thể.

3. Cho hệ mật mã dạng affine xác định thông qua công thức: $y=x * k + l \bmod 26$; trong đó x,y là vị trí ký tự trong bảng chữ cái tiếng Anh (A ở v.tr. 0, B v.tr. 1…, Z v.tr. 25); khóa là cặp số (k,l). Số lượng giá trị khóa (k,l) thực sự phân biệt là: **(6pt)**
   a) 260 b) 300 c) 312 d) 360 e) 338 f) Khác

*Đáp án: c, có 12*312 khả năng cho cặp (k,l); lưu ý k phải là số ntcn với 26 nên chỉ có 12 khả năng*

4. Giả sử hệ thống phân cấp các cơ quan CA ở một nước X được tổ chức dạng như một đồ thị cây (có CA trung ương ở gốc của cây này) có chiều cao tối đa là 5, và cây này có 100 nút lá. Cho biết khi 2 bên A và B đăng ký vào 2 CA khác nhau trong cây này thì số lượng tối đa (X) các phép kiểm tra xác thực certificate phải làm để A có thể xác thực khóa công khai của B là bao nhiêu? **(6pt)**
   a) 5 b) 100 c) 101 d)10 e) 9 f) Khác

Đáp án: e hoặc d đều chấp nhận được; trong cây phân cấp này các nút kề nhau đều phát hành chứng chỉ KCK cho nhau nên số lượt kiểm tra tối đa sẽ bằng độ dài đường dẫn kết nối A và B có du di thêm 1-2 bước kiểm tra.

5. Tại sao nói thủ tục bắt tay ba bước trong giao thức TCP là điểm yếu dễ tấn công? Nêu các nguyên nhân đúng – **Đa lựa chọn (ĐLC - 3pt)**
   a) Thiết kế "ngây thơ" về ATTT; b) THiết kế lúc Internet chưa tồn tại; c) Pha bắt tay thiếu xác thực;
   d) Pha bắt tay không làm chữ ký số; e) Các gói SYN quá to; f) Thiếu chứng chỉ số;

Đáp án: a,b,c đều đúng.

6. Phân tích điểm yếu của việc xây dựng hệ điều khiển truy nhập dựa trên khái niệm ma trân điều khiển ACM bằng đúng 3 câu: **(5pt)**

Đáp án: ACM là lớn nên tốn kém tài nguyên nhớ, chưa kể rất nhiều trường rỗng; việc lưu toàn bộ là không cần thiết mà có thể phân rã để tiết kiệm bộ nhớ và xử lý hiệu quả hơn; phân theo dòng hay theo cột là phổ biến nhất.

7. Alice xây dựng hệ RSA cho mình dựa trên 2 số nguyên tố (p &q) có kích thước là 50 và 100 chữ số còn Cathy xây dựng với 2 số có độ dài 60 và 70 chữ số. Hãy so sánh có phân tích về tính an toàn giữa 2 trường hợp này. Bên nào tốt hơn, cho 1-2 câu phân tích: **(5pt)**

Đáp án: Dường như với giải pháp của Alice thì tốt hơn vì n lớn hơn tuy nhiên khi kẻ địch tiến hành thử PTTSNT thì sẽ sớm tìm ra p (số nhỏ) trước ➔ giải pháp của Cathy tốt hơn.

8. Những nhận định nào về mã xác thực thông điệp MAC và mã CRC-32 là đúng **- (ĐLC-3pt)**
   a) MAC an toàn hơn ; b) CRC-32 an toàn hơn c) MAC cho phép quản lý tài nguyên
   d) Mục đích khác nhau; e) Mục đích có nhiều điểm chung

Đáp án: a,d,e

9. Khi nào cần đặt tường lửa bảo vệ liên mạng: **(2pt)**

a) Khi liên kết tài nguyên của cơ quan trong mạng nội bộ b) Khi cần hệ thống phòng chống virus

c) Khi thường xuyên kết nối từ mạng nội bộ ra mạng Internet d) Khi hệ điều hành theo DAC thay vì MAC

Đáp án: c.

10. Bộ lọc gói trong bảo vệ có chức năng : **(2pt)**

a) Lọc các luồng dữ liệu với những thuộc tính lựa chọn để cho đi qua hệ thống bảo vệ.

b) Lọc những thông tin có trong dữ liệu được mã hóa cho đi qua tường lửa.

Đáp án: a.

11. Phương pháp mã hóa nào được sử dụng để mã hóa khóa bí mật khi thiết kế "phong bì điện tử"? **(2pt)**

a) thuật toán mã hoá đối xứng b) thuật toán mã hóa không đối xứng

Đáp án: b.

12. Mạng riêng ảo (VPN) dùng để: **(2pt)**

a) Bảo vệ việc kết nối của mạng nội bộ và các máy tính cá nhân tới mạng Internet khỏi các tác động trái phép từ bên ngoài.

b) Bảo vệ dữ liệu trong quá trình truyền qua mạng mở.

Đáp án: b

13. Giao thức nào được xây dựng để hỗ trợ cho hệ thống giao dịch điện tử của ngân hàng dùng thẻ ? **(2pt)**

a) S/MIME b) SET c) IPSEC d) TLS 1.0

Đáp án: b.

14. Để xác định tính hiệu lực của chứng thư số, ta phải sử dụng những cơ chế nào dưới đây ? **(ĐLC-3pt)**

a) Chính sách an ninh tích hợp; b) Chính sách chứng thư số;

c) Danh sách chứng thư bị thu hồi; d) Các tên miền hết hiệu lực

Đáp án: c.

15. Mô hình tin cậy PKI nào có thể được sử dụng giữa CA và các CA cấp dưới: **(3pt)**

a) Mô hình chứng thực chéo; b) Mô hình phân cấp;

c) Mô hình bắc cầu; d) Mô hình liên kết.

Đáp án: b

16.Phương pháp mã hóa nào không phải là mã hóa đối xứng ? **(2pt)**

a) DES b) El-Gamal c) RC5 d) IDEA

Đáp án: b.

17. Mô hình Bell-LaPadulla có 2 luật viết tát là ? **(2pt)**

a) "No Read Up" & "No Write Down"; b) "No Read Down" & "No Write Up" c) "Read Up" & "Write Down"

Đáp án: a.

18.Thuật toán DES dựa trên cấu trúc nào? **(2pt)**
a) cấu trúc Feistel; b) mã hóa dòng; c) kiến trúc SQUARE

Đáp án: a.

19. Nhận định nào về RBAC là đúng: **(3pt)**

a) Mô hình có tính trực giác cao, tính đại biểu, hỗ trợ cái gọi là "đặc quyền tối thiểu"

b) Là thừa kế có chọn lọc từ mô hình DAC và MAC, trong đó khát niệm vai trò khái quát hóa khái niệm nhóm

c) Thể hiện quan hệ thừa kế giữa các phiên bản mô hình theo thời gian: $RBA_0 \rightarrow RBA_1 \rightarrow RBA_2 \rightarrow RBA_3$

Đáp án: a.

20. Thuật toán RSA thuộc dạng nào của thuật mã hóa(xét trên phương diện an toàn) ? **(2pt)**

a) An toàn vô điều kiện b) An toàn chứng minh được c) An toàn thực tiễn

Đáp án: b hoặc c.

PHẦN ĐỀ TỰ LUẬN: Giao thức an toàn và ứng dụng

Với mỗi sinh viên, trước hết em hãy xác đinh cho mình giá trị X (MSSV mod 2) =

Y (<Hàng chục của MSSV> mod 2) = (Ví dụ: MSSV 201432456 ➔ X=0, Y=1)

Trong một giờ học về ATTT, thầy Lâm giới thiệu 1 giao thức đơn giản cơ bản PRT_AU (xem dưới đây) và yêu cầu sinh viên bàn luận nhóm để phân tích mục đích & phê bình ưu-nhược; từ đó thử thiết kế một giao thức làm tốt hơn hoặc có lợi ích hơn về một phương diện nào đó. Kết quả cuối giờ có 4 sinh viên loại khá-giỏi là An, Bình, Chi, Dũng đã đưa ra các phiên bản mới dưới đây.

PRT_AU: (thầy Lâm nêu đầu giờ)

1) A→S: ID_A
2) S→A: Password Request
3) A→S: $H(PW_A)||T$

PROT_00: (của An)

1) A→S: ID_A
2) S→A: R
3) A→S: $H(PW_A||R)$

PROT_10: (của Bình)

1) A→S: ID_A
2) S→A: R
3) A→S: $H(PW_A||R)$
4) S→A: $\{k_s\}p_A$

PROT_01: (của Chi)

A→S: ID_A || $H(PW_A||T)$ || T

PROT_11: (của Dũng)

1) A→S: ID_A
2) S→A: R
3) A→S: $\{R+1\}p_A$
4) S→A: $\{k_s\}p_A$ where $p_A = H(PW_A)$

Trong đó một số ký hiệu sử dụng ở trên có ý nghĩa như sau:

ID_A – là ID (danh tính) của A; R là 1 số ngẫu nhiên; T là một nhãn thời gian (Timestamp) tại thời điểm hiện thời (có thể sử dụng computer clock)

PW_A là chuỗi ký tự mật khẩu của A; p_A là giá trị băm của mật khẩu của A, tức là $p_A = H(PW_A)$ và với H là một hàm băm xác định công bố trước.

Câu hỏi:

1. Phân tích rõ mục đích của PRT_AU và từ đó so sánh với PROT_0X để thấy rõ ưu nhược điểm.

Đáp án: Mục đích của giao thức PRT_AU là xác thực danh tính (trong đăng nhập) bằng mật khẩu.

Tuy nhiên hệ thống (S) chỉ cần lưu giá trị băm của mật khẩu mà thôi.

Khi phân tích sự khác biệt với giải pháp của An hay Chi, cần nêu rõ là giải pháp PRT_AU yếu hơn vì có vẻ như sử dụng timestamp để chống tấn công phát lại nhưng không thành công vì kẻ địch hoàn toàn có thể tạo fake T kết hợp với $H(PW_A)$ *đã nghe trộm. Trong khi đó GP của An/Chi đều có thể chống được replay attack: của An thì sử dụng cơ chế thách thức-đáp ứng với số ngẫu nhiên R, còn của Chi thì đưa T vào trong băm nên không thể can thiệp. Cả 2 giải pháp này S luôn lưu chữ chính mật khẩu của A (chứ không phải chỉ giá trị băm).*

2. Phân tích chỉ rõ sự khác biệt và tính năng mới của PROT_1Y so với hai giao thức ở câu trên (1)

Đáp án: Điểm mới chung so với PRT_AU là xác thực với cơ chế thách thức-đáp ứng với sử dụng giá trị ngẫu nhiên R – giá trị luôn luôn thay đổi không lặp lại qua các phiên chạy của giao thức, vì thế không cho phép kẻ địch có thể thực hiện tấn công phát lại theo cách phát lại bản ghi cũ một cách tầm thường. Lưu ý rằng giải pháp của Bình vẫn cần S lưu giá trị mật khẩu gốc của người sử dụng còn giải pháp của Dũng thì S chỉ cần lưu giá trị băm của mật khẩu. Tính năng mới (và cũng là điểm khác biệt chính với PROT_0X) là giao thức PROT_1Y *cho phép tạo ra khóa phiên mới cho NSD là A có thể dùng luôn để kết nối bằng mật mã với hệ thống trong phần trao đổi thông tin hoặc dữ liệu tiếp theo.*

3. Thầy Lâm sau đó trình bày một phiên bản nâng cao khác và thách thức lớp phân tích và tìm ra vấn đề còn tồn tại.
    1) $A \rightarrow S: ID_A \,||\, ID_B \,||\, r_1$
    2) $S \rightarrow A: \{ID_A \,||\, ID_B \,||\, r_1 \,||\, k_s \,||\, \{ID_A \,||\, k_s \,||\, r_1\} p_B\} p_A$
    3) $A \rightarrow B: \{ID_A \,||\, k_s \,||\, r_1\} p_B$
    4) $B \rightarrow A: \{r_2\} k_s$
    5) $A \rightarrow B: \{r_1 + r_2\} k_s$

    Sinh viên Đạt đã trả lời tốt câu hỏi của thầy, phân tích đúng vấn đề tồn tại và tìm ra giải pháp khắc phục thành công, trong đó chỉ cần thực hiện 1 sửa đổi ở bước 5 mà thôi.

    Em hãy phân tích mục đích của giao thức và thử đoán xem vấn đề tồn tại mà Đạt chỉ ra? Nếu có thể hãy chỉ ra giải pháp khắc phục cũng như ý tưởng giải quyết của Đạt.

Đáp án: Giao thức này được thiết kế nhằm mục đích là thực hiện tạo khóa phiên cho A và B thông qua hỗ trợ của S (tất nhiên bao hàm sự xác thực của S đối với A) và có hy vọng chống được tấn công của kẻ địch biết khóa phiên cũ (đã từng dùng). Ý tưởng của người thiết kế là ngay cả khi kẻ địch có khóa phiên cũ cũng sẽ không thể đáp ứng được thành công (ở bước 5) do không biết r1. Tuy nhiên kẻ địch nham hiểm có thể đã ghi chép toàn bộ các thông điệp trong quá khú, do đó có thể truy vết các thông điệp đã dùng với khóa phiên cũ và từ đó dễ dàng tìm ra được r1 (các em hãy thử nghĩ thêm tại sao?). Chính điều này Đạt là điểm yếu đã phát hiện ra được. Từ đó đưa ra giải pháp khắc phục để che giấu r1, chẳng hạn như dùng băm trong bước 5 (em hãy tự tìm cách cụ thể hóa).