Một số câu hỏi ôn tập
(đã từng dùng làm đề thi trong các năm trước)

*Chú ý: Sinh viên Việt-Nhật không cần quan tâm đến các câu có dấu ***

1. Viết 1-3 câu để giải thích các khái niệm:
   Cryptography
   Cryptanalysis
   Known-plaintext only attack
   Confusion
   Difusion
   Exhautive key searching (tìm kiếm khoá vét cạn)
2. Phân biệt một hệ mã thường (coding system) và một hệ mật mã (cipher system). Cho ví dụ.
3. ** Độ dư thừa của ngôn ngữ là gì. Cho ví dụ. Tại sao nói độ dư thừa ảnh hưởng đến tính an toàn của một hệ mật mã.
4. ** Khái niệm IC và cách phá giải mã Vigenere
5. Xét monoalphabetic substitution cipher với bảng chữ cái tiếng Anh, khoá được chọn ngẫu nhiên. Cho biết:

a) Chiều dài khoá của hệ mã này là gì?
b) Có phải tất cả các khoá này đều an toàn như nhau không? Tại sao?
c) Kích thước khoá của mật mã nhân tính? Mật mã affine?

6. Phân biệt ATBM vô điều kiện (tuyệt đối) và thực dụng
7. Xét thuật toán DES. Cho biết:

a) Các thuộc tính của S-box và ý nghĩa của chúng
b) Tại sao nói việc xây dựng thuật toán cần dựa trên số vòng lặp càng lớn càng tốt?
c) Sơ đồ khối của DES chuẩn có bao nhiêu vòng lặp? Vẽ sơ đồ với 1 vòng lặp và mô tả chức năng các phần?
d) Xét DES có 2 vòng lặp. Vẽ sơ đồ sinh mã và giải mã. Giải thích tại sao sơ đồ giải mã biến đổi nghịch đảo với sinh mã.
e) Cho biết các điểm yếu của DES

8. So sánh các chế độ sử dụng mã khối ECB và CBC
9. Cho p=7, q=11 và e=7 trong hệ RSA. Hãy thực hiện các công việc sau:

a) Xác định khoá công khai và bí mật của hệ
b) Tính MÃ của TIN X=2
c) Nếu sử dụng hệ này để làm chữ ký, xác định chữ ký cho X nói trên
d) Khi nào thì TIN không thể đem mã hoá trực tiếp? Giả sử lúc này TIN được đem chia thành các khối và chữ ký được tạo thành bằng cách ký lên từng khối riêng biệt rồi ghép lại. Cho biết kích thước của khối này theo bit? Hãy trình bày nhược điểm của hệ chữ ký này? Hãy cho biết một giải pháp khắc phục.

10. Cho một vecto mang như sau: a' = (3, 5, 9, 18)

a) Vector này có phải là siêu tăng hay không, tại sao?
b) Dựa trên vector này bạn hãy xây dựng một hệ khoá công khai theo phương pháp của Merkle-Hellman (nguyên tắc từ bài toán đóng thùng)
c) Cho một TIN x = (1,0,1,1), bạn hãy sử dụng hệ khóa công khai vừa xây dựng ở trên để tính mã y từ x
d) Với giá trị y tìm được ở câu trên, hãy cho biết cách giải mã để thu được tin x ban đầu.

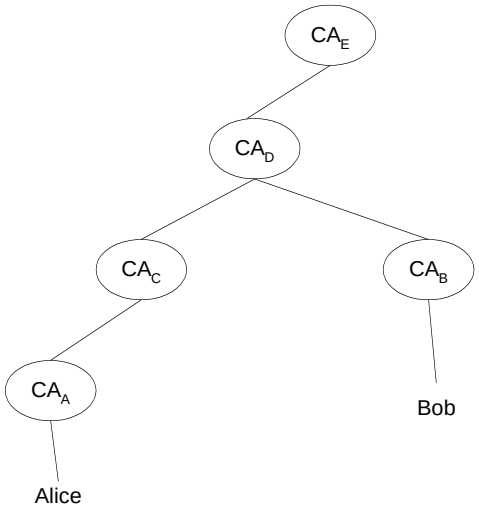
11.

a) Cho biết hai thuộc tính cần thiết của các hàm băm được sử dụng trong các hệ chữ ký điện tử.
b) Giải thích ý nghĩa của 2 thuộc tính này đối với an toàn của hệ DS
c) Vẽ các sơ đồ khối của bộ sinh chữ ký và kiểm định chữ ký, trong đó chữ ký có độ dài cố định là d bits.
d) Khái niệm đụng độ. Ý nghĩa của nghịch lý Birthday?

12. Cho ví dụ về phương pháp trao chuyển khoá Diffie-Hellman. Tại sao nói phương pháp này chưa an toàn? Kẻ địch có thể tấn công như thế nào?

13.

a) Sơ lược mô tả khái niệm certificate trong PKC
b) ứng dụng của certificate là gì?
c) Xét một certificate tree như hình vẽ sau. Mô tả vai trò của các CA và cho biết cấu trúc cây này hoạt động như thế nào?



14. Sau đây là thuật toán trao chuyển khoá Needham-Schroeder:

1) $A \rightarrow S$: A, B, R_A

2) $S \rightarrow A$: $E_{K_{AS}}$ (R_A, B, K, $E_{K_{BS}}$ (K,A))

3) $A \rightarrow B$: $E_{K_{BS}}$ (K,A)

4) $B \rightarrow A$: E_K (R_B)

5) $A \rightarrow B$: E_K (R_B-1)

Trong đó K_{XY} là khoá đối xứng bí mật giữa X và Y, R_X là số ngẫu nhiên sinh ra bởi X và khoá K bí mật cần thiết lập giữa A và B. Cho biết:

a) Môi trường trong đó giao thức này được sử dụng và mục đích của giao thức.
b) Giải thích ý nghĩa từng bước của giao thức.

15.

a) Thủ tục bắt tay 3 bước Needham-Schoeder
b) ** Giao thức truyền tin bí mật không trao chuyển khoá (Shamir)
c) ** ZKP là gì? Cho ví dụ.

16. Thế nào là off-line password guessing. Hãy cho biết phương pháp và kỹ thuật để chống lại. Giả sử 1 hệ thống khi chưa được trang bị theo phương pháp này bị kẻ địch đột nhập và thử thành công sau 50 giây chạy chương trình của nó; vậy cần thiết kế lại hệ thống như thế nào để vẫn kẻ địch trên không thể làm được như vậy trong vòng 10 tiếng.

17. IC có quy luật liên hệ gì với văn bản mà từ đó nó được tính ra. Hãy thử nêu một ước lượng so sánh giữa IC của các hệ mã sau đây:

Additive cipher	Multiplicative cipher
Vernam cipher	DES
One-time-pad cipher	Homophonic substitution cipher với ví dụ trong giáo trình

Vigenere cipher với ví dụ trong giáo trình

Hãy vắn tắt biện luận về sự phán đoán của mình

18. Số ngẫu nhiên thường được sử dụng trong các cryptographic protocol. Bạn có nhận xét gì về điều này. Minh hoạ bằng việc nêu một protocol cụ thể đã học và nêu rõ trong đó số ngẫu nhiên đã được sử dụng với công dụng cụ thể như thế nào.

19. Hãy nghiên cứu một bài toán thực tế như sau:
Một trường đại học có một máy chủ Unix mạnh với rất nhiều terminal bố trí ở các địa điểm công cộng (thư viện, phòng thí nghiệm, nhà ăn ...) để sinh viên có thể truy nhập và sử dụng các dịch vụ cài đặt sẵn trong đó có truy nhập Internet.
Nhà Sách của nhà trường mở dịch vụ bán sách trên Internet, tạo khả năng cho sinh viên có thể truy nhập tới danh mục sách qua trang Web, lựa chọn sách cần thiết, gửi yêu cầu mua (order) của mình và số thẻ credit card để thanh toán.

Cụ thể là một sinh viên, tên Alice, sẽ phải thực hiện các bước sau đây để mua sách:
+ Vào một terminal nào đó và đăng nhập vào máy chủ.
+ Cô ta chọn một Web Browser nào đó, ví dụ Netscape, để truy nhập đến trang Web của Nhà Sách và lựa chọn sách muốn mua
+ Cô ta ra lệnh để thực hiện việc gửi yêu cầu mua sách cùng với số thẻ credit card của mình qua mạng Internet đến Nhà Sách đó.

<u>*Yêu cầu*</u>:
a) Hãy cho biết và mô tả vắn tắt ít nhất ba mối đe doạ an toàn (security threat) trong scenario nói trên
b) Đối với mỗi mối đe doạ thử nếu một phương pháp và cách cài đặt cụ thể để phòng tránh.

20. ** Trong ví dụ thuật toán Zero-Knowledge-Protocol đã học ở chương 6
a) Hãy giải thích ý nghĩa của việc sử dụng số ngẫu nhiên $b \in \{0,1\}$
b) Giả sử Victor luôn luôn tiến hành lặp đi lặp lại các bước của protocol đúng 10 lần. Giả sử Eve có thể nghe trộm các cuộc liên lạc giữa Peggy và Victor. Bạn hãy đánh giả khả năng (xác xuất) để Eve có thể mạo danh thành công giả làm Peggy trong protocol với Victor. Giải thích.

21. Phân biệt Discretionary Access Control và Mandatory Access Control. Nêu một số ví dụ ứng dụng phổ biến của mỗi phương pháp. Access Control matrix có được sử dụng trong phương pháp thứ hai hay không?

22. Mô tả một hệ thống truy nhập có ứng dụng one-time password

23. Mô tả/phân tích một loại lỗ hổng an ninh đối với online database khi kẻ địch có thể khiến server đáp ứng các các câu hỏi truy vấn SQL ngoài dự kiến và phá vỡ tính an toàn của hệ thống.

24. Mô tả DDoS SYN attack đối với tầng TCP. Có thể sử dụng firewall để hạn chế tấn công này như thế nào.

25. Một hệ chữ ký điện tử dùng hàm băm được chế tạo theo phương pháp áp dụng SKC (với sơ đồ mã móc xích CBC) cụ thể là dùng DES. Được biết hệ chữ ký này đã bị một hãng cạnh tranh tấn công và tạo ra được hai văn bản khác nhau có cùng chữ ký trong vòng một ngày. Hãy cho biết cách cải tiến để sao cho hãng kẻ thù nói trên vẫn dùng kỹ thuật và phương tiện như cũ sẽ phải mất đến 3 năm mới có thể thành công. Hãy nêu biện luận và tính toán chi tiết của mình.