ĐÁP ÁN

Bài 1

Câu hỏi tự luận

Câu 1.

- Lỗ hổng:
  - Không có bức tường lửa
  - Cấu hình phần cứng phần mềm không đúng
  - Không có phần mềm phòng chống virus
  - Không backup dữ liệu
  - Mật khẩu lưu ở dạng tường minh
- Nguy cơ:
  - Lộ thông tin mật
  - Xâm nhập trái phép vào máy chủ
  - Dùng công nghệ xã hội dò tìm mật khẩu
  - Virus, sâu và các phần mềm có hại
  - Không ai dám tra tiền trên Website thương mại vì sợ lộ thông tin tài khoản
- Tấn công
  - Xem trộm dữ liệu tài khoản
  - Từ chối đã trả tiền mua bằng credit card
  - Giả mạo người khác đăng tin
  - Sửa thông tin trên trang Web
  - Tấn công từ chối dịch vụ của Website bán hàng cạnh tranh

Câu 2.

- Để đáp ứng nhu cầu an ninh của các tổ chức doanh nghiệp một cách hiệu quả và để đánh giá, lựa chọn các chính sách an ninh khác nhau, người quản trị cần có cách tiếp cận hệ thống để xác định yêu cầu an ninh và thể hiện các cách tiếp cận đáp ứng các yêu cầu đó.
- Bộ phận chuẩn truyền thông thuộc Hiệp hội truyền thông quốc tế ITU-T (International Telecommunication Union đã định nghĩa cách tiếp cận hệ thống đó trong X800 - kiến trúc an ninh mạng bao gồm các khái niệm an ninh như tấn công, cơ chế, dịch vụ an ninh.
- RFC 2828– Requests Functionalty Comments là tài liệu thuật ngữ an ninh Internet "Internet Security Glossary", ở trên trang URL: http://www.rfc- editor.org/**rfc**/**rfc2828**.txt

Câu 3.

- Cơ chế an ninh chuyên dụng được cài đặt trong một giao thức của một tầng vận chuyển nào đó: mã hoá, chữ ký điện tử, quyền truy cập, toàn vẹn dữ liệu, trao đổi có phép, đệm truyền, kiểm soát định hướng và chứng nhận.
- Cơ chế an ninh phổ dụng không chỉ rõ được dùng cho giao thức trên tầng nào hoặc dịch vụ an ninh cụ thể nào mà cung cấp chức năng tin cậy cho một tiêu chuẩn nào đó, nhãn an ninh chứng tỏ đối tượng có tính chất nhất định, phát hiện sự kiện, vết theo dõi an ninh, khôi phục an ninh.

Câu 4.

- Bảo mật: ai đó đọc thông tin mật của bạn như mật khẩu, thư riêng tư.
- Toàn vẹn: một sinh viên xâm nhập vào máy chủ của Trường để thay đổi điểm thi
- Sẵn sàng: Tấn công từ chối dịch vụ, gửi quá nhiều yêu cầu lên máy chủ Web

- Xác thực: email với tên người gửi sai
- Chống từ chối: một người nào đó đã mua trực tuyến một số cổ phiếu sau đó lại từ chối
- Kiểm soát quyền truy cập: Hacker vào tiếm quyền của người quản trị

Câu 5.

- Xác thực thực thể đầu cuối: sử dụng với kết nối logic để tin tưởng định danh kết nối
- Xác thực dữ liệu gốc: khi truyền dữ liệu không kết nối, nó cung cấp bằng chứng về nguồn gốc dữ liệu đã tuyến bố

Câu 6.

- Bảo mật kết nối: bảo vệ dữ liệu người dùng trong kết nối đó.
- Bảo mật không kết nối: bảo vệ dữ liệu người dùng trên một khối dữ liệu
- Bảo mật một trường được chọn: bảo mật một trường trong dữ liệu người dùng
- Bảo mật luồng truyền: bảo mật thông tin tránh việc dò tìm trên đường truyền.

Câu 7.

- Toàn vẹn kết nối có khôi phục: phát hiện sửa, chèn, xoá, trì hoãn dữ liệu, tìm cách khôi phục
- Toàn vẹn kết nối không khôi phục: chỉ phát hiện sửa, chèn, xoá, không khôi phục
- Toàn vẹn không kết nối: phát hiện sửa và có thể trì hoãn một gói tin duy nhất
- Toàn vẹn với một trường lựa chọn: toàn vẹn một trường nào đó trong dữ liệu

Câu 8.

- Chống từ chối gốc: có bằng chứng chứng minh người đó đã gửi thông điệp
- Chống từ chối đích: Chứng minh thông điệp đã được nhận bởi người nhận

Câu 9.

Trên mô hình ta thấy có các điểm yếu sau:

- Nơi gửi người gửi là ai, xác thực anh ta như thế nào: tài khoản - mật khẩu,
- Trên đường truyền bị xem trộm hoặc sửa nội dung: mã hoá, tính toàn vẹn
- Nơi nhận: đúng người nhận không, có thể mở được nội dung để đọc không: quyền truy cập, trọng tài chuyển khóa mật xác thực hai bên
- Hai đầu không được từ chối đã gửi và đã nhận: chữ ký điện tử, chống từ chối

Câu 10.

- Vượt trái phép qua hàm canh cổng xâm nhập vào hệ thống thông tin lấy thông tin trái phép, sửa đổi, phá hoại phần mềm, phần cứng, các tiến trình.
- Hàm canh cổng cần phải có chức năng phát hiện kẻ xâm nhập trái phép, ngăn chặn chúng hoặc cảnh báo cho hệ thống thông tin.

Bài tập trắc nghiệm

1. d;	**2.** c;	**3.** b;	**4.** d;	**5.** a;	**6.** d;	**7.** b.
8. c;	**9. d;**	**10. c; d**	**11. c**	**12. d**	**13. d**	**14. d**
15. c;						

Bài 2

Bài tập 2 trắc nghiệm:

1. b;	**2.** b;	**3.**	**4.**	**5.**	**6.**	**7.**
8.	**9.**	**10.**	**11.**	**12.**	**13.**	**14.**
15.						

Bài 3

Câu hỏi tự luận

Câu 1.

- N đóng với cộng, nhân; N không đóng với trừ và chia
- Z đóng với cộng, nhân, trừ; N không đóng với chia
- P đóng với cộng, trừ, nhân, chia và đếm được
- R đóng với cộng, trừ, nhân, chia và không đếm được

Câu 2.

Thuật toán Euclid để tính ước chung lớn nhất của 2 số. Nó lặp việc thay số bằng cặp số nhỏ và phần dư của số lớn theo số nhỏ, cho đến khi 1 số bằng 0, thì số kia là Ước chung lớn nhất.

Câu 3.

Số n là số nguyên tố, thì trên tập các đại diện Z_n ta có thể thực hiện các phép toán: cộng, trừ, nhân và chia cho số khác 0. Vì khi đó mọi số đều có số nghịch đảo.

Câu 4.

Số nguyên tố là số chỉ ước là 1 và chính nó. Muốn phân tích một số ra tích lũy thừa của các thừa số nguyên tố, ta phải xét tính chia hết của nó và các thương nhận được cho từng số nguyên tố từ nhỏ đến lớn.

Câu 5

Hai số nguyên tố cùng nhau là hai số có ước chung lớn nhất bằng 1. Dùng thuật toán Euclid để kiểm tra hai số có nguyên tố cùng nhau không.

Câu 6

Thuật toán Euclid mở rộng tính ước chung lớn nhất và tính nghịch đảo trong trường hợp 2 số nguyên tố cùng nhau. Nó giống như tiến hành đồng thời nhiều thuật toán Euclid cùng một lúc.

Câu 7

Giá trị hàm Euler của 1 số là số các số nguyên tố cùng nhau với số đó mà nhỏ hơn nó.

Câu 8.

Tính giá trị hàm Euler dựa vào định nghĩa đếm số các số nguyên tố cùng nhau với số đó và nhỏ hơn nó hoặc tìm phân tích của số đó ra thừa số là lũy thừa của các số nguyên tố, rồi tính giá trị hàm Euler dựa vào phân tích đó.

Câu 10.

Định lý Euler là mở rộng của Ferma, vì nếu một số p là nguyên tố, thì nó sẽ nguyên tố cùng nhau với mọi số nhỏ hơn nó và giá trị hàm Euler của p bằng p-1.

Câu 13.

Định lý phần dư Trung hoa dùng để đưa việc tính toán số học Modulo theo số lớn về việc tính toán số học modulo theo số nhỏ, nếu có thể phân tích số lớn thành tích các số nhỏ nguyên tố cùng nhau. Định lý này cũng giúp giải hệ phương trình modulo.

Câu 14.

Xem bài giảng: căn nguyên thủy của một số là số nguyên tố cùng nhau với số đã cho mà lũy thừa của nó tạo nên tập các số nguyên tố cùng nhau với số đó.

Câu 15.

Để tính logarit rời rạc, ta phải tính lần lượt các lũy thừa của cơ số theo modulo, rồi so sánh với giá trị logarit cần tính.

Câu 16.

Xem bài giảng: Logarit rời rạc theo modulo n là bài toán ngược của bài toán lũy thừa, nhưng khó hơn nhiều, thường đòi hỏi cơ số là căn nguyên thủy của n và số lấy logarit cũng là nguyên tố cùng nhau với n

Bài tập 3 trắc nghiệm:

1. d; **2.** d; **3.** d; **4.** c; **5.** d; **6.** b; **7.** c.
8. d; **9.** d; **10.** b; **11.c** **12.d** **13.d** **14.c**
15. b **16.c** **17.c**

Bài tập ôn tập:

1. a. 51 = 3.15 + 6; Do đó theo định nghĩa: 51 mod 15 = 6
   b. -51 =-4.15 + 9; Vậy: (-51) mod 15 = 9
2. a. 215 mod 29 = 12; Do đó theo định nghĩa: 12 là đại diện của 215 theo modulo 29
   b. -158 mod 29 = 29 – 158 mod 29 = 29 – 13 = 16
3. Các lớp tương đương và đại diện modulo 13:

-26	-25	-24	-23	-22	-21	-20	-19	-18	-17	-16	-15	-14
-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
13	14	15	16	17	18	19	20	21	22	23	24	25

Hàng viết đậm từ 0 đến 12 gồm các đại diện của modulo 13.

4. Quan hệ tương đương đồng dư: hai số có quan hệ đồng dư theo modulo n, nếu chúng có cùng số dư khi chia cho n:
   a) 101 ≡ 36 mod 13? – Đúng
   b) -101 ≡ -36 mod 13? – Sai
   c) 165 ≡ 34 mod 65? - Sai
   d) -165 ≡ 30 mod 65? - Đúng
5. Lập bảng nhân theo modulo 11, nêu các cặp nghịch đảo nhau trong bảng.

Bảng nhân modulo 11

X	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	8	2	6	10	3	4
5	0	5	10	4	8	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	11	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Các cặp sau nghịch đảo nhau theo modulo 11, vì chúng có tích theo modulo bằng 1:
(1, 1), (2, 6), (3, 4), (4, 3), (5, 9), (6, 2), (7, 8), (8, 7), (9, 5), (10, 10)

6. Bạn có thể thay các số bằng các số tương đương theo mod n bất cứ lúc nào trong các công thức cộng, trừ, nhân theo modulo:

$(a \pm b) \bmod n = [a \bmod n \pm b \bmod n] \bmod n$ (**)

$(a.b) \bmod n = [a \bmod n . b \bmod n] \bmod n$ (***)

a. Áp dụng tính chất (**):

$(74 - 215) \bmod 9 = -141 \bmod 9 = 9 - 141 \bmod 9 = 9 - 6 = 3$

hay $(74 \bmod 9 - 215 \bmod 9) \bmod 9 = (2 - 8) \bmod 9 = -6 \bmod 9 = 3$

b. Áp dụng tính chất (***):

$(244 . 315) \bmod 250 = (244 \bmod 250 . 315 \bmod 250) \bmod 250$

$= ((-6) \bmod 250 . 65 \bmod 250) \bmod 250 = (-6 .65) \bmod 250 =$

$(-390) \bmod 250 = 250 - 390 \bmod 250 = 250 - 140 = 110$

c. Áp dụng Áp dụng tính chất (***):

$(144.315 - 265.657) \bmod 51 = (144.315 \bmod 51 - 265.657 \bmod 51) \bmod 51$

$= (-9.9 \bmod 51 - (10.(-6)) \bmod 51) \bmod 51 = (-81 + 60) \bmod 51 =$

$-21 \bmod 51 = 51 - 21 \bmod 51 = 30$

7. Dùng định nghĩa tìm nghịch đảo

a. $6^{-1} \bmod 11 = 2$, vì $6.2 \bmod 11 = 1$

b. $5^{-1} \bmod 11 = 9$, vì $9.5 \bmod 11 = 1$

c. $6^{-1} \bmod 13 = 11$, vì $(-2).6 \bmod 13 = 1$

d. $12^{-1} \bmod 13 = (-1)^{-1} \bmod 13 = -1 \bmod 13 = 12$

e. $(n-1)^{-1} \bmod n = n-1$

f. $13^{-1} \bmod 15 = (-2)^{-1} \bmod 15 = -8 \bmod 15 = 7$

g. $21^{-1} \bmod 25 = (-4)^{-1} \bmod 15 = 6$

8. Áp dụng thuật toán Euclid:

2110 = 1 x 1945 + 165 gcd(1945, 165)
1945 = 11 x 165 + 130 gcd(165, 130)
165 = 1 x 130 + 35 gcd(130, 35)
130 = 3 x 35 + 25 gcd(35, 25)
35 = 1 x 25 + 10 gcd(25, 10)
25 = 2 x 10 + 5 gcd(10, 5)
10 = 2 x 5 + 0 gcd(5, 0)

Vậy ta có ước chung cần tìm là 5:

GCD(2110, 1945) = GCD(5, 0) = 5

9. $845^{-1} \bmod 2011 = ?$ Ta sử dụng thuật toán Euclid mở rộng để tìm nghịch đảo.

Q	A1	A2	A3	B1	B2	B3
—	1	0	2011	0	1	845
2	0	1	845	1	–2	321
2	1	–2	321	–2	5	203
1	–2	5	203	3	–7	118
1	3	-7	118	-5	12	85

1	-5	12	85	8	-19	33
2	8	-19	33	-21	50	19
1	-21	50	19	29	-69	14
1	29	-69	14	-50	119	5
2	-50	119	5	129	-307	4
1	129	-307	4		426	1

Vậy 845^{-1} mod 2011 = 426 mod 2011= 426

10. Dùng Định lý phần dư Trung hoa tính
11. Dùng Định lý Ferma
    a. $5^{12}(\text{mod } 13) = 1$
    b. $8^{13}(\text{mod } 13) = 8$
    c. $10^{100}(\text{mod } 17) = (10^{16})^6 . 10^4(\text{mod } 17) = 9^2 \text{mod } 17 = 13$
    d. $15^{125}(\text{mod } 19) = (15^{18})^7.15^{-1}(\text{mod } 19) = 14$

Hàm Euler. Hàm Euler của một số n là số các số nguyên tố cùng nhau với n và nhỏ hơn n.

N	Φ(n)	Điều kiện
P	P - 1	p nguyên tố
p^n	$p^n - p^{n-1}$	p nguyên tố
s.t	Φ(s).Φ(t)	s, t nguyên tố cùng nhau
p.q	(p-1)(q-1)	p, q hai nguyên tố khác nhau

12. Tính giá trị hàm Euler:
    a) $\Phi(23) = 22$
    b) $\Phi(55) = \Phi(5.11) = \Phi(5).\Phi(11) = 4.10 = 40$
    c) $\Phi(180) = \Phi(4.5.9) = \Phi(4).\Phi(5).\Phi(9) = \Phi(2^2).\Phi(5).\Phi(3^2) = (2^2-2).4.(3^2-3) = 48$
    d) $\Phi(200) = \Phi(8.25) = \Phi(2^3).\Phi(5^2) = (2^3-2^2).(5^2-5) = 80$
    e) $\Phi(900) = \Phi(4.9.25) = \Phi(4).\Phi(9).\Phi(25) = \Phi(2^2).\Phi(3^2).\Phi(5^2) = (2^2-2).(3^2-3).(5^2-5) = 2.6.20 = 240$
    f) $\Phi(6300) = \Phi(7.900) = \Phi(7).\Phi(900) = 6.240 = 1440$
13. Tính:
    a) 4^8 mod 15= 1, vì Φ(15) = 8, gcd(4, 15) = 1.
    b) 11^9 mod 20= 10, vì Φ(20) = 8, gcd(11, 20) = 1
    c) 12^{402} mod 25= 19, vì Φ(25) = 20, gcd(12, 25) = 1, 402 = 20.20 + 2,
    d) 12^{402} mod 25= $12^{400}.12^2$mod 25= 144 mod 25 = 19
    e) 135^{162} mod 64= $(135 \text{ mod } 64)^{32.5+2}$ mod 64 = 7^2mod 64=49, vì $\Phi(64) = \Phi(2^6) = 64 - 32 = 32$
    f) 335^{453} mod 23= $(335 \text{ mod } 23)^{22.20+13}$ mod 23 = 5^{13}mod 23 =$5^8.5^4.5$mod 23 = 16.4.5 mod 23 = 21, vì Φ(23) = 22
    g) $(3/7)^8$ mod 10=$(3.7^{-1})^8$mod 10 = $(3.3)^8$ mod 10 = $(-1)^8$ mod 10 = 1

14. Theo thuật toán lũy thừa dựa trên biểu diễn nhị phân của số mũ n: $11^{23} \bmod 187$

$23 = 16 + 4 + 2 + 1$; $23_2 = 10111$

$11^{23} \bmod 187 = (((1^2.11)^2)^2.11)^2.11)^2.11) \bmod 187$

15. Trên thực tế tính toán bằng tay được dựa trên phép lặp bình phương và nhân với cơ số

$11^{23} \bmod 187 = 11^{16}.11^4.11^2.11 \bmod 187$

$11^2 \bmod 187 = 121$

$11^4 \bmod 187 = 121^2 \bmod 187 = 55$

$11^8 \bmod 187 = 55^2 \bmod 187 = 3025 \bmod 187 = 33$

$11^{16} \bmod 187 = 33^2 \bmod 187 = 1089 \bmod 187 = 154$

$11^{23} \bmod 187 = 11^{16}.11^4.11^2.11 \bmod 187 = (154.55.121.11) \bmod 187$
$= (-33.(-66).5.11.11) \bmod 187 = 3.6.5.11^4 \bmod 187 = 3.6.5.55 \bmod 187$
$= 265 \bmod 187 = 88$

16. Kiểm tra căn nguyên thủy

a. a = 2 có phải là căn nguyên thủy của 7 không? $\Phi(7) = 6$

$2 \bmod 7 = 2$; $2^2 \bmod 7 = 4$; $2^3 \bmod 7 = 1$;

$3 < 6 = \Phi(7)$, vậy 2 không là căn nguyên thủy của 7.

b. a = 2 có phải là căn nguyên thủy của 11 không? $\Phi(11) = 10$

$2 \bmod 11 = 2$; $2^2 \bmod 11 = 4$; $2^3 \bmod 11 = 8$;
$2^4 \bmod 11 = 5$; $2^5 \bmod 11 = 10$; $2^6 \bmod 11 = 9$,
$2^7 \bmod 11 = 7$; $2^8 \bmod 11 = 3$; $2^9 \bmod 11 = 6$, $2^{10} \bmod 11 = 1$

Vậy 2 là căn nguyên thủy của 11.

c. a = 3 có phải là căn nguyên thủy của 11 không? $\Phi(11) = 10$

$3 \bmod 11 = 3$; $3^2 \bmod 11 = 9$; $3^3 \bmod 11 = 5$;
$3^4 \bmod 11 = 4$; $3^5 \bmod 11 = 1$;
$5 < 10 = \Phi(11)$, vậy 3 không là căn nguyên thủy của 11.
Ta lấy ví dụ một số cặp (số nguyên tố, căn nguyên thủy) sau:
(3, 2); (5, 2); (7, 3), (11, 2); (13, 6); (17, 10); (19, 10); (23, 10)

17. Tìm Logarit rời rạc:

a) $x = \log_2 5 \bmod 11 = 4$

$2^0 \bmod 11 = 1$; $2^1 \bmod 11 = 2$; $2^2 \bmod 11 = 4$;
$2^3 \bmod 11 = 8$; $2^4 \bmod 11 = 5$;

b) $x = \log_2 5 \bmod 13 = 9$

$2^0 \bmod 13 = 1$; $2^1 \bmod 13 = 2$; $2^2 \bmod 13 = 4$;
$2^3 \bmod 13 = 8$; $24 \bmod 13 = 3$; $2^5 \bmod 13 = 6$;
$2^6 \bmod 13 = 12$; $2^7 \bmod 13 = 11$; $2^8 \bmod 13 = 9$;
$2^9 \bmod 13 = 5$;

c) $x = \log_3 7 \bmod 13 = ?$

$3^0 \bmod 13 = 1$; $3^1 \bmod 13 = 3$; $3^2 \bmod 13 = 9$;
$3^3 \bmod 13 = 1$,

Vô nghiệm (3 không phải là căn nguyên thủy của 13).

18. Trong khi lũy thừa là bài toán dễ dàng, thì bài toán logarit rời rạc là bài toán khó.

Bài 4

Bài tập 4 trắc nghiệm:

1. c;	**2.** d;	**3.** c;	**4.** d;	**5.** a.	**6.** d;	**7.** b;
8. d;	**9.c**	**10.a**	**11.a**	**12.a**	**13. c, d.**	

Bài tập ôn tập:

1. c;	**2.** c;	**3.** c;	**4.** d;	**5.** b;	**6.** d;	**7.** c.
8. a;	**9.** c;	**10.** b;	**11.c**	**12.c**		

Bài 5

Câu hỏi tự luận

Câu 1. Sử dụng mã công khai ta có thể làm được các việc sau mà mã đối xứng không thể:

- Tách vai trò người gửi người nhận, vi 2 khóa là khác nhau
- Kết hợp với bản băm tạo được chữ ký điện tử, tức là xác nhận được tính toàn vẹn của thông điệp và danh tính người gửi. Góp phần chống từ chối người gửi.
- Trao đổi khóa Diffie-Hellman cho phép 2 người sử dụng trao đổi một cách công khai khóa mật dùng chung giữa hai người.

Câu 2.

Như ta biết dùng mã khóa đối xứng như DES, AES có thể bảo mật nội dung thông điệp. Nhưng nó không thể giúp xác thực tính toàn vẹn thông điệp và tính pháp lý của người gửi. Mã công khai dễ dàng đáp ứng được hai yêu cầu sau.

Câu 3.

Ví dụ RSA dựa vào cặp bài toán: nhân 2 số nguyên tố lớn là dễ và bài toán ngược lại là phân tích một số thành tích của 2 số nguyên tố. Đây là bài toán khó, tương đương với bài toán phân tích một số ra lũy thừa các thừa số nguyên tố hay tính giá trị hàm Euler của một số rất lớn. Còn trong trao đổi khóa Diffie-Hellman thì bài toán thuận dễ là bài toán lũy thừa, còn bài toán nghịch khó là bài toán logarit rời rạc.

Câu 5.

Vì người đó biết được hai tham p, q, nên dễ dàng áp dụng được Định lý phần dư Trung Hoa tính mã và giải mã qua modulo p và q, thay vì qua modulo n.

Câu 6. Tấn công RSA về mặt toán học có 3 dạng

- Phân tích N = p.q, sau đó tính Φ(N) và d
- Tìm n trực tiếp Φ(N) và tính d
- Tìm d trực tiếp

Hiện tại tin rằng tất cả đều tương đương với bài toán phân tích là bài toán khó, giải rất lâu với n đủ lớn cỡ 1024 bit.

Câu 7

Làm sao 2 người không thể gặp nhau, chỉ sử dụng môi trường mạng không an toàn, mà có thể trao đổi khóa mật dùng chung được (Khóa mật này sẽ dùng để mã hóa thông điệp thường bằng mã đối xứng). Ở đây không sử dụng trọng tài tin cậy thư ba, hai người sử dụng muốn trao đổi trực tiếp với nhau. Bối cảnh này sẽ thúc đẩy việc ứng dụng Internet an toàn trong mọi lĩnh vực. Diffie-Hellman để xuất mỗi người có một khóa riêng và một khóa công khai. Mọi người đều có thể tự tính khóa dùng chung với một người khác bất kỳ, bằng cách sử dụng khóa riêng của mình và khóa công khai của người khác đó.

Câu 9. Xác thực mẩu tin liên quan đến các khía cạnh sau khi truyền tin trên mạng

- Bảo vệ tính toàn vẹn của mẩu tin: bảo vệ mẩu tin không bị thay đổi hoặc có các biện pháp phát hiện nếu mẩu tin bị thay đổi trên đường truyền.
- Kiểm chứng danh tính và nguồn gốc: xem xét mẩu tin có đúng do người xưng tên gửi không hay một kẻ mạo danh nào khác gửi.
- Không chối từ bản gốc: trong trường hợp cần thiết, bản thân mẩu tin chứa các thông tin chứng tỏ chỉ có người xưng danh gửi, không một ai khác có thể làm điều đó. Như vậy người gửi không thể từ chối hành động gửi, thời gian gửi và nội dung của mẩu tin.

Câu 10. Có 3 cách là mã hoá, mã xác thực MAC và bản băm hash. Mã hóa đối xứng không tách người gửi với người nhận và không biết sự thay đổi của thông điệp, mã công khai không chỉ rõ được bản tin có toàn vẹn hay không, như bị cắt bớt trọn vẹn một câu. MAC là vừa nén vừa dùng khóa chia sẻ giữa người gửi và người nhận. Nó được đính kèm để người nhận dùng lại thuật toán MAC và so sánh nhận biết sự thay đổi của thông điệp. Nhưng MAC không tách được vai trò người gửi, người nhận và thuật toán MAC ít công khai, nhiều khi chỉ cần xác thực tính toàn vẹn, nên không cần khóa, có thể công khai, do đó người ta dùng hàm băm.

Câu 11.

Định lý phần dư Trung hoa dùng để đưa việc tính toán số học Modulo theo số lớn về việc tính toán số học modulo theo số nhỏ, nếu có thể phân tích số lớn thành tích các số nhỏ nguyên tố cùng nhau. Định lý này cũng giúp giải hệ phương trình modulo.

Câu 12.

Nghịch lý ngày sinh nhật là thông thường ta nghĩ trong lớp có hơn 366 người thì chắc chắn có ít nhất 2 người trùng ngày sinh nhật theo nguyên lý lồng chim ồ câu. Nếu thay điều kiện chắc chắn bằng xác suất để có 2 người trùng ngày sinh nhật lớn hơn hoặc bằng 0.5, thì ta nghĩ ngay là lớp phải có khoảng 183 = 366/2. Nhưng trên thực tế, con số đó ít hơn rất nhiều, chỉ là 23 người. Như vậy, xác xuất để hai bản tin có trùng bản băm là không nhỏ như ta nghĩ, chính vì vậy phải tăng độ dài bản băm lên và tìm thuật toán băm khó sao cho việc tìm ra hai bản tin có cùng bản băm là rất khó.

Câu 13. Thuật toán băm SHA1:

- Chia thành các khối, mỗi khối 512 bit
- Xử lý từng khối, thực hiện 80 bước lặp, sử dụng 160 bit véc tơ đầu vào tác động, cho ra kết quả 160 bit bản băm của khối
- Khối đầu sử dụng 160 bit véc tơ ban đầu
- Các khối sau lấy 160 bit của khối trước làm véc tơ đầu vào
- 160 bit đầu ra của khối cuối cùng sẽ là bản băm của toàn bộ thông điệp.

Câu 14

Xem thêm bài giảng. Chữ ký điển tử của một người sử dụng trên một mẩu tin tại một thời điểm xác định được xem như nén mẩu tin về một kích thước cố định và được xác thực bởi một số thông số đặc trưng như bản băm mẩu tin, thông tin mật người gửi, số ngẫu nhiên của lần ký gửi đó. Nó cung cấp các khả năng để

- Kiểm chứng tác giả, ngày và giờ ký
- Xác thực nội dung mẩu tin
- Được kiểm chứng bởi bên thứ 3 để chống từ chối

Câu 15

Mỗi lần ký nó dùng một số ngẫu nhiên đặc trưng cho lần ký đó, vì cùng một mẩu tin trong các lần ký khác nhau sẽ cho ra các chữ ký khác nhau.

Câu 16

Người nhận sẽ nén mẩu tin lại cũng theo thuật toán qui định chung. Sau đó dùng thuật toán, bản băm, chữ ký điện tử nhận được tính toán kiểm tra chữ ký. Nếu đúng, thì cho ta tin tưởng rằng mẩu tin không bị sửa và đúng là người gửi ký. Nếu sai, thì có một số nguyên nhân: mẩu tin bị

sửa, người ký không phải là người như đã tuyên bố hoặc chữ ký này đã bị sử dụng lại không đúng của lần ký này.

Bài tập 5 trắc nghiệm:

1. c;	**2.** c;	**3.** c;	**4.** d;	**5.** d;	**6.** c;	**7.** c.
8. d;	**9.** c;	**10.** b;	**11.c**	**12.c**	**13.d**	**14.a**
15. b	**16.b**	**17.c**	**18.b**	**19.b**	**20.a**	

Bài tập 5 ôn tập:

11. b	**12.c**	**13. d**	**14. c**

Bài 6

Câu hỏi tự luận

1. Ưu nhược điểm của việc quản lý khóa công khai bằng thư mục công cộng: cho phép nhập tên và khóa công khai với Thư mục; có thể thay khóa bất cứ lúc nào; Thư mục được in định kỳ và có thể truy cập qua mạng. Mô hình trên vẫn còn có các lỗ hổng để kẻ xâm nhập sửa hoặc giả mạo khi vào hệ thống.
2. Ưu nhược điểm của việc quản lý khóa công khai bằng chủ quyền khóa công khai: Đăng ký khóa công khai gống như với thư mục, sau đó người dùng nhận được bất kỳ khóa công khai mong muốn nào một cách an toàn, bằng cách truy cập thời gian thực đến Thư mục khi cần đến khóa. Yêu cầu truy cập thời gian thực là một nhược điểm.
3. Ưu nhược điểm của việc quản lý khóa công khai bằng chủ quyền chứng nhận khóa công khai: chứng nhận cho phép trao đổi khóa không cần truy cập thời gian thực đến Chủ quyền thư mục khóa công khai. Để làm việc đó chứng nhận trói danh tính của người sử dụng với khóa công khai của anh ta và "đóng dấu và giấy chứng nhận" đó để tránh giả mạo.
4. Giải thích sơ đồ trao đổi trực tiếp khóa mật dùng chung bằng khóa công khai: A tạo ra một cặp khóa công khai mới tạm thời; A gửi B một khóa công khai và danh tính của họ; B tạo ra khóa phiên và gửi nó cho A sử dụng khóa công khai được cung cấp; A giải mã khóa phiên và cả hai cùng dùng nó. Nhược có thể dùng thông điệp cũ, nên cần bổ sung nhãn thời gian vào các thông điệp.
5. Giải thích sơ đồ trao đổi khóa mật dùng chung bằng phương pháp kết hợp dùng khóa công khai với sự hỗ trợ của bên thứ ba: Trung tâm chia sẻ khóa chính (master key) với mỗi người sử dụng. Và phân phối khóa phiên sử dụng khóa chính với Trung tâm. Sơ đồ khóa công khai được dùng để phân phối khóa chính. Sơ đồ ba lớp này đặc biệt hữu ích khi người sử dụng phân tán rộng
6. Mục đích dùng khóa chính và khóa phiên là gì? Thời gian sử dụng chúng khác nhau như thế nào: Khóa phiên (section key): Khóa tạm thời, dùng để mã hoá dữ liệu giữa nhóm người sử dụng, cho một phiên logic và sau đó bỏ đi. Khóa chính (master key): dùng để mã các khóa phiên, chia sẻ giữa người sử dụng và trung tâm phân phối khóa.
7. Nêu các vấn đề gặp phải khi giải quyết bài toán phân phối khóa: Thời gian sống của khóa bộ phận cần được hạn chế để cho an toàn hơn. Sử dụng phân phối khóa tự động thay mặt người dùng, nhưng phải có hệ thống tin cậy, các khóa cấp phát được sinh ra càng ngẫu nhiên càng tốt. Cần phải có hệ thống phân phối khóa phân tán và phân cấp
8. Nêu mục đích và yêu cầu của hệ thống Kerberos: xác thực trung tâm với yêu cầu: an toàn, tin cậy, trong suốt, có thể mở rộng.
9. Nêu cấu tạo mô hình Kerberos và việc yêu cầu dịch vụ trong lãnh địa khác được thực hiện như thế nào: là sơ đồ xác thực dùng bên thứ ba và có máy chủ xác thực (AS –

Authentication Server). Người dùng thỏa thuận với AS về danh tính của mình, AS cung cấp sự tin cậy xác thực thông qua thẻ cấp thẻ TGT (Ticket Granting Ticket). Người sử dụng thường xuyên yêu cầu TGS cho truy cập đến các dịch vụ khác dựa trên thẻ cấp thẻ TGT của người sử dụng. Và máy chủ cung cấp thẻ (TGS – Ticket Granting Server) cung cấp các thẻ dịch vụ theo yêu cầu và thẩm quyền.

10. Mô tả giao thức xác thực sử dụng dịch vụ trong hệ thống Kerberos: gồm 11 bước xem trong bài giảng.
11. Kerberos phiên bản 5 có những cải tiến gì, giải thích quá trình sinh khóa từ mật khẩu: nó cung cấp những cải tiến so với phiên bản 4, cụ thể hướng tới các thiếu xót về môi trường, thuật toán mã, thủ tục mạng, thứ tự byte thông điệp, thời gian sử dụng thẻ, truyền tiếp xác thực, xác thực lãnh địa con. Và các sự khác biệt về kỹ thuật như: mã kép dùng mã hai lần thẻ bằng khóa mật của máy chủ đích và khóa riêng của người sử dụng, khắc phục các dạng sử dụng không chuẩn trong phiên bản trước, khóa phiên được mã bằng khóa xác thực của TGS cộng thêm với yếu tố thời gian của lần sử dụng, chống tấn công mật khẩu. Xem bài 8: trước hết, xâu mật khẩu s được lưu dạng các ký tự 7 bit, sau đó cuộn gọn lại nhờ phép XOR thành 56 bit; lấy nó làm 56 bit khóa của DES, bổ sung thành 64 bit khóa gồm 8 khối 8 bit, mật khẩu gốc được mã theo chế độ mã móc nối dây chuyền với khóa được tạo ở trên. kết quả nhận được khóa 64 bit sinh ra từ mật khẩu
12. Mô tả hoạt động của cơ sở hạ tầng khóa công khai PKI: quản lý danh tính người sử dụng (NSD) với khóa công khai của người đó; cấp chứng nhận của Chủ quyền Giấy chứng nhận CA cho NSD; Huỷ và Thu hồi các giấy chứng nhận không còn hiệu lực; Tạo ra các Thư mục để lưu trữ các chứng nhận và danh sách thu hồi (CRL); Cung cấp dịch vụ sẵn sàng cung cấp cho NSD như: đăng ký, truy cập, xin giấy chứng nhận, đưa ra danh sách thu hồi CRL.
13. Nêu các nhiệm vụ an ninh chính của Hệ thống thư điện tử: nâng cao an toàn thư điện tử là mục đích quan trọng của mọi hệ thống trao đổi thư. Ở đây phải đảm bảo các yêu cầu sau: tính bảo mật nội dung tin gửi, xác thực người gửi mẩu tin, tính toàn vẹn của mẩu tin, hơn nữa bảo vệ khỏi bị sửa, tính chống từ chối gốc, chống từ chối của người nhận.
14. Giải thích sơ đồ bảo mật thư điện tử: xem bài giảng
15. Giải thích sơ đồ xác thực thư điện tử: xem bài giảng
16. Mô tả các bước gửi một bức thư điện tử: xem bài giảng
17. Mô tả các bước nhận một bức thư điện tử: xem bài giảng

Bài tập 6 trắc nghiệm:

1. a;	**2. d**;	**3.** c;	**4. c**;	**5. b**;	**6. d**;	**7.** c.
8. c;	**9. b**;	**10. c**;	**11.a**	**12.c**	**13.c**	**14.b**
15. c	**16.b**	**17.d**	**18.c**	**19.c**	**20.**	

Bài 7

Câu hỏi tự luận

1. Nêu một số ứng dụng của Ipsec và lợi ích khi dùng Ipsec: nó cung cấp: xác thực, bảo mật và quản trị khoá. IPSec được dùng trên mạng LAN, mạng WAN riêng và chung và trên cả mạng Internet. Nó cung cấp: xác thực, bảo mật và quản trị khoá. IPSec được dùng trên mạng LAN, mạng WAN riêng và chung và trên cả mạng Internet. Lợi ích của IPSec: Khi IPSec được cài đặt trên bức tường lửa/router, nó cung cấp an toàn mạnh cho mọi việc truyền tin qua vành đai. IPSec nằm dưới tầng vận chuyển nên trong suốt với mọi ứng dụng. IPSec có thể trong suốt với người sử dụng đầu cuối. Nó cũng có thể cung cấp an toàn cho người sử dụng riêng biệt, khi họ truy cập từ xa đến mạng của công ty hay cần thiết lập mạng ảo an toàn trong công ty cho một số ứng dụng quan trọng.

2. Nêu kiến trúc của Ipsec: Tiêu đề xác thực (AH – Authentication Header) là tiêu đề mở rộng dùng cho xác thực; Bao bọc tải trọng bảo mật (ESP – Encapsulating Security Payload) là tiêu đề mở rộng dùng cho mã hóa.
3. Các dịch vụ mà IPsec có thể cung cấp trên tầng IP là gì: IPSec nhằm đạt các mục đích sau: kiểm soát truy cập, toàn vẹn không kết nối, xác thực nguồn gốc dữ liệu, từ chối tải lại gói (đây là một dạng của toàn vẹn liên kết từng phần), bảo mật (mã hoá), bảo mật dòng lưu lượng giới hạn.
4. Liên kết SA được định danh duy nhất bởi bộ ba thuộc tính nào, liệt kê các tham số SA: Chỉ số các tham số bảo mật (SPI): là xâu bit gắn với liên kết, nó cho phép hệ thống nhận tin lựa chọn liên kết để xử lý; địa chỉ IP đích; định danh giao thức bảo mật: chỉ rõ liên kết là AH hay ESP; chỉ số dãy (sequence number), thông tin về tiêu đề xác thực và tiêu đề mở rộng AH & EH, thời gian sống. Có lưu trữ cơ sở dữ liệu của các liên kết an toàn.
5. Nêu các trường của Tiêu đề xác thực AH: Next Header; Payload Length; Reserved; SPI - chỉ số các tham số bảo mật xác định liên kết bảo mật; Sequence Number - dãy số (32 bit): giá trị đếm đơn điệu tăng, dùng để phát hiện việc gửi lại bản sao của một gói tin nào đó; Authentication Data – giá trị dùng để kiểm tra tính toàn vẹn của gói dữ liệu nhận được.
6. Nêu định dạng gói tin IP4 và IP6 trước và sau khi áp dụng AH trong chế độ vận chuyển: xem bài giảng.
7. Nêu định dạng gói tin IP4 và IP6 trước và sau khi áp dụng AH trong chế độ đường hầm: xem bài giảng
8. Nêu định dạng của giao thức Bao bọc tải trọng bảo mật ESP:
    a. Chỉ số các tham số bảo mật (SPI) : xác định liên kết an toàn.
    b. Sequence Number - dãy số (32 bit):giá trị đếm đơn điệu tăng, dùng để phát hiện việc gửi lại bản sao của một gói tin nào đó.
    c. Payload Data – dữ liệu tải trọng là gói tin (trong chế độ vận chuyển) hoặc gói IP (trong chế độ đường hầm) được mã hóa.
    d. Padding – bộ đệm dùng để bổ sung vào bản rõ trước kho mã hóa.
    e. Độ dài bộ đệm
    f. Tiêu đề tiếp theo
    g. Dữ liệu xác thực là trường có độ dài thay đổi chứa giá trị kiểm tra tính toàn vẹn được tính dựa vào toàn bộ ESP trừ trường dữ liệu xác thực.
9. Mô tả chế độ vận chuyển và đường hầm của ESP:

Chế độ vận tải được sử dụng để mã và tuỳ chọn xác thực dữ liệu IP:

- Dữ liệu được bảo vệ nhưng phần đầu vẫn để rõ để biết địa chỉ đích. Nếu lựa chọn xác thực sẽ có thêm ESP Authentication Data.
- Kẻ phá hoại vẫn có thể phân tích vận chuyển một cách hiệu quả
- Là lựa chọn tốt đối với ESP máy chủ vận chuyển tới máy chủ.

Chế độ ống mã toàn bộ gói IP

- Bổ sung tiêu đề mới, có thể thêm phần xác thực nếu lựa chọn.
- Tại mỗi cổng chuyển tiếp trung gian sẽ kiểm tra và xử lý tiêu đề IP và các phần rõ, còn giữ nguyên phần mã hóa.

Tốt cho mạng riêng ảo VPN (Virtual Private Network), cổng đến cổng an toàn

10. Mô tả 4 trường hợp kết hợp an ninh cơ bản: xem bài giảng
11. Nêu các mối đe dọa an ninh Web:
    a. Tính toàn vẹn: sửa đổi dữ liệu, ngựa thành Toroa, thay đổi bộ nhớ.
    b. Bảo mật: theo dõi trên mạng, do thám từ máy chủ hay trạm, theo dõi luồng thông tin xem máy trạm nào liên hệ với máy chủ.
    c. Từ chối dịch vụ: xóa luồng của người sử dụng, làm tràn máy với các đe dọa, làm tràn bộ nhớ, cô lập máy để từ chối dịch vụ.
    d. Xác thực: giả mạo người dùng hợp pháp, giả mạo dữ liệu.
12. Nhiệm vụ an ninh của SSL là gì:

a. Xác thực máy chủ: Cho phép người sử dụng xác thực được máy chủ muốn kết nối. Lúc này, phía browser sử dụng các kỹ thuật mã hóa công khai để chắc chắn rằng chứng chỉ và khóa công cộng của máy chủ là có giá trị và được cấp phát bởi một CA trong danh sách các CA đáng tin cậy của máy trạm.
b. Xác thực máy trạm: Cho phép phía máy chủ xác thực được người sử dụng muốn kết nối. Phía máy chủ cũng sử dụng các kỹ thuật mã hóa công khai để kiểm tra xem chứng chỉ và khóa công cộng của máy chủ có giá trị hay không và được cấp phát bởi một CA trong danh sách các CA đáng tin cậy không.
c. Mã hóa kết nối: Tất cả các thông tin trao đổi giữa máy trạm và máy chủ được mã hóa trên đường truyền nhằm nâng cao khả năng bảo mật.

13. Nêu kiến trúc SSL. Có hai lớp giao thức; Giao thức bản ghi SSL ở dưới và ở lớp trên là các giao thức: bắt tay, thay đổi đặc tả mã, cảnh báo và HTTP
14. Mô tả thủ tục Bản ghi SSL: Bước đầu tiên là chia gói, sau đó nén lại. Tiếp theo tính MAC của bản nén và đính kèm, ở đây khóa mật chung được sử dụng. Rồi mã hóa và bổ sung tiêu đề SSL.
15. Mô tả thủ tục Bắt tay SSL:

Thủ tục này cho phép máy chủ và máy trạm:

- Xác thực nhau
- Thỏa thuận thuật toán mã hóa và MAC
- Thỏa thuận khóa mã sẽ dùng

Nó bao gồm bốn giai đoạn trao đổi một loạt thông tin:

- Thiết lập các khả năng bảo mật
- Xác thực máy chủ và trao đổi khoá
- Xác thực máy trạm và trao đổi khoá
- Kết thúc việc trao đổi

16. Nêu các yêu cầu an ninh của Thanh toán điện tử an toàn SET:
    a. Trao đổi an toàn giữa các đối tác
    b. Tin tưởng vì sử dụng giấy chứng nhận X509v3
    c. Riêng biệt vì hạn chế thông tin vừa đủ cho những người tham gia giao dịch.
17. Nêu trình tự các sự kiện trong Thanh toán điện tử: 7 bước trong bài giảng.
18. Mô tả chữ ký kép trong SET: Người mua tạo chữ ký kép trên
    - Thông tin đơn đặt OI cho người bán
    - Thông tin trả tiền PI cho ngân hàng

Không bên nào biết chi tiết của người khác. Nhưng cần phải biết là họ được kết nối với nhau. Sử dụng chữ ký kép cho mục đích này: Ký trên bản ghép của OI và PI, ở đây H là hàm băm, KR_C là khóa riêng của chủ thẻ:

19. Nêu sơ đồ người mua gửi yêu cầu trả tiền:

a. Trong thông tin yêu cầu của người mua bao gồm phần gửi cho người bán và phần thông qua người bán chuyển tiếp cho cổng trả tiền. Phần gửi cho người bán có đơn mua hàng, chữ ký kép, giấy chứng nhận của chủ thẻ và bản băm của hóa đơn trả tiền.
b. Phần gửi chuyển cho cổng trả tiền gồm bản mã của khóa phiên được mã bằng khóa công khai của ngân hàng và bản mã của hóa đơn trả tiền được mã bằng khóa phiên.

20. Nêu sơ đồ chứng nhận trả tiền:

a. Kiểm chứng mọi chứng nhận
b. Giải mã phong bì điện tử của khối giấy phép và nhận được khóa đối xứng, sau đó giải mã khối giấy phép
c. Kiểm tra chữ ký của người bán trên khối giấy phép
d. Giải mã phong bì điện tử khối trả tiền, nhận được khóa đối xứng, sau đó giải mã khối trả tiền
e. Kiểm tra chữ ký kép trên khối trả tiền

f. Kiểm tra rằng, thanh toán ID nhận được từ người bán phù hợp với danh tính trong PI nhận được (không trực tiếp) từ người bán
g. Yêu cầu và nhận được giấy phép từ nơi phát hành
h. Gửi trả lời giấy phép cho người bán

Bài tập 7 trắc nghiệm:

1. d;	**2. b**;	**3. b**;	**4. d**;	**5. a**;	**6. b**;	**7. d**.
8. b;	**9. c**;	**10. d**;	**11.b**	**12.a**	**13.c**	**14.d**
15. b	**16.d**	**17.b**	**18.d**	**19.d**	**20.c**	

Bài 8
Câu hỏi tự luận

1. Hãy phân loại kẻ xâm nhập vào hệ thống và lấy ví dụ minh họa:
   a. Kẻ giả danh
   b. Kẻ lạm quyền
   c. Người sử dụng giấu mặt

   Nêu các ví dụ tương ứng
2. Nêu một số kỹ thuật xâm nhập hay được sử dụng:
   a. Tìm mục tiêu và thu thập thông tin
   b. Truy cập ban đầu
   c. Leo thang quyền
   d. Lần vết khôi phục
3. Việc đoán mật khẩu thường được xảy ra theo những kịch bản nào:
   a. Mặc định, mật khẩu ngắn, tìm kiếm các từ chung
   b. Thông tin của người dùng (thay đổi tên, ngày sinh, số điện thoại, các mối quan tâm và từ chung)
   c. Tìm kiếm tổng thể mọi khả năng của mật khẩu
   d. Theo dõi qua vai khi nhập password
   e. Sử dụng chương trình ngựa thành Toroa để thu thập thông tin về mật khẩu
4. Nêu một số cách tiếp cận để phát hiện kẻ xâm nhập:

   Phát hiện thống kê bất thường
   a. Vượt qua ngưỡng thống kê nào đó của các sự kiện
   b. Dựa trên mô tả của các hành vi

   Dựa trên qui tắc
   c. Phát hiện hành động bất thường dựa trên qui tắc được xây dựng từ các mẫu sử dụng trước
   d. Định danh thâm nhập: sử dụng hệ chuyên gia
5. Giải thích cách dùng việc kiểm tra và phân tích bản ghi để phát hiện kẻ xâm nhập:
   a. Công cụ cơ bản để phát hiện xâm nhập là kiểm tra bản ghi đơn giản
   b. Một phần của hệ điều hành đa người sử dụng
   c. Sẵn sàng để sử dụng, có thể không có thông tin trong định dạng mong muốn
   d. Số đếm, đo, thời gian khoảng, sử dụng nguồn. Sử dụng các kiểm tra khác nhau trên số liệu phân tích để xác định hành vi hiện tại có chấp nhận được không
   e. Tính kỳ vọng, phương sai, biến nhiều chiều, chuỗi thời gian,…
6. Nêu một số phương pháp phát hiện kẻ xâm nhập dựa trên qui tắc:
   a. Phân tích các bản ghi kiểm tra cũ để xác định mẫu sử dụng và qui tắc tự sinh
   b. Quan sát hành vi hiện tại và sánh với các qui tắc để nhận thấy nếu nó phù hợp
   c. Giống như phát hiện thống kê bất thường không đòi hỏi kiến thức biết trước về sai lầm an toàn
   d. Sử dụng công nghệ hệ chuyên gia, định danh sự thâm nhập dựa vào qui tắc

e. Với qui tắc định danh sự xâm nhập đã biết, các mẫu điểm yếu, hoặc các hành vi nghi ngờ
f. So sánh các bản ghi kiểm tra hoặc các trạng thái theo qui tắc
g. Qui tắc được sinh bởi các chuyên gia

7. Có các biện pháp hỗ trợ nào để tạo mới mật khẩu một cách an toàn:
   a. Là bảo vệ tuyến đầu chống kẻ xâm nhập
   b. Người sử dụng được cung cấp cả hai:
      i. Login – xác định đặc quyền của người sử dụng
      ii. Password – xác thực danh tính của họ
   c. Passwords thường được lưu trữ dạng mã hoá
      i. Unix sử dụng DES lặp
      ii. Các hệ thống gần đây sử dụng hàm hash
   d. Cần phải bảo vệ file passwords trong hệ thống
8. Bạn hãy nêu nguyên lý tạo khóa từ mật khẩu trong Kerberos 5:
   a. Trước hết, xâu mật khẩu s được lưu dạng các ký tự 7 bit, sau đó cuộn gọn lại nhờ phép XOR thành 56 bit
   b. Lấy nó làm 56 bit khóa của DES, bổ sung thành 64 bit khóa gồm 8 khối 8 bit
   c. Mật khẩu gốc được mã theo chế độ mã móc nối dây chuyền với khóa ở trên.
   d. Kết quả nhận được khóa 64 bit sinh ra từ mật khẩu
9. Bạn hãy nêu một số kiểu phần mềm có hại: cửa sập, bom logic, ngựa thành Tơ roa, virus, sâu, Zombie
10. Nêu các biện pháp chống virus:
    - Biện pháp tốt nhất là ngăn ngừa,
    - Phát hiện virus nhiễm trong hệ thống
    - Định danh loại virus nhiễm
    - Loại bỏ khôi phục hệ thống về trạng thái sạch
11. Mô tả sơ đồ hệ miễn dịch số, nêu các bước điển hình trong hoạt động của nó:
    a. Chương trình giám sát trên mỗi PC sử dụng nhiều kiểu tìm tòi dựa trên hành vi của hệ thống, theo dõi sự thay đổi chương trình hay chữ ký tập thể để phát hiện virus. Sau đó nó gửi bản sao đến máy điều hành.
    b. Máy điều hành lấy mẫu gửi đến máy phân tích virus trung tâm.
    c. Máy này tạo môi trường để máy nhiễm có thể chạy để phân tích. Sau đó nó tạo ra đơn để định danh và loại bỏ virus
    d. Đơn được gửi trả lại máy điều hành.
    e. Máy điều hành gửi lại đơn cho máy bị nhiễm
    f. Đơn được gửi tới các máy khác trong tổ chức hệ thống
    g. Những người khác ngoài tổ chức sẽ nhận được bản cập nhật chống virus để chống virus mới đó.
12. Nêu cách chống tấn công từ chối dịch vụ từ xa: có ba cách bảo vệ sau đây được dùng rộng rãi
    a. Ngăn ngừa tấn công và chiếm lĩnh trước.
    b. Phát hiện tấn công và lọc trong quá trình sử dụng dịch vụ
    c. Lần vết nguồn tấn công và xác định sự tấn công sau khi sử dụng xong dịch vụ.
    d. Nói chung có phạm vi rộng các khả năng tấn công, vì vậy phải có nhiều biện pháp chống và sử dụng kết hợp chúng.
13. Mô tả ma trận kiểm soát quyền truy cập:
    a. Chủ thể - thực thể chủ động (NSD, quá trình) có khả năng truy cập đối tượng
    b. Đối tượng - thực thể bị động (file hoặc chương trình, đoạn trong bộ nhớ) được truy cập đến
    c. Quyền truy cập – cách mà đối tượng được truy cập bởi chủ thể

d. Cột ứng với đối tượng gồm danh sách quyền truy cập đến nó của các chủ thể định danh
e. Hàng ứng với chủ thể gồm các thẻ về khả năng truy cập của nó đến các đối tượng

14. Mô tả mô hình hệ thống tin cậy Bell LaPadula:

Một trong những mô hình an toàn nổi tiếng nhất. Được cài đặt như các chính sách bắt buộc trong hệ thống. Có hai chính sách chính

- Không đọc lên (tính chất an toàn đơn giản): chủ thể chỉ có thể đọc các đối tượng nếu mức độ an toàn hiện tại của chủ thể trội hơn phân loại an toàn của đối tượng
- Không viết xuống: chủ thể chỉ có thể bổ sung/viết lên đối tượng nếu mức độ an toàn hiện tại của chủ thể nhỏ hơn hoặc bằng mức phân loại của đối tượng

Bài tập 8 trắc nghiệm:

1. d;	**2. b**;	**3. a**;	**4. c**;	**5. a**;	**6. d**;	**7. a**.
8. d;	**9. b**;	**10. d**;	**11.b**	**12.d**	**13.b**	**14.d**
15. b	**16.d**	**17.d**	**18.c**	**19.b**		