EXAM questions for the course TTM4135 - Information Security
June 2010

Part 1

This part consists of 6 questions all from one common topic. The number of maximal points for every correctly answered question is given next to the question. Maximal number of points in this part of the exam is 28. Time for work on this test: ~60 minutes.

TOPIC: Classic symmetric cryptographic techniques

1. (6 points) Construct a table for the Playfair Cipher with the keyword EFFECTIVENESS?
2. (6 points) Encrypt the phrase: "EXAMFORINFORMATIONSECURITY"
3. (6 points) Decrypt the sequence: "PQFVCKFUFBGMUFYSTIKZKAGWWG"
4. (5 points) Explain how "Caesar Cipher" works!
5. (5 points) Explain what is "One-time pad"

KEY for Part 1

TOPIC:

1.

E	F	C	T	I
V	N	S	A	B
D	G	H	K	L
M	O	P	Q	R
U	W	X	Y	Z

2.

EX	AM	FO	RI	NF	OR	MA	TI	ON	SE	CU	RI	TY

↓

CU	VQ	NW	ZB	GN	PM	QV	IE	WG	VC	EX	ZB	AT

3.

PQ	FV	CK	FU	FB	GM	UF	YS	TI	KZ	KA	GW	WG

↓

OP	EN	TH	EW	IN	DO	WE	XA	CT	LY	AT	NO	ON

= OPEN THE WINDOW EXACTLY AT NOON

4. Student should mention that the Caesar cipher is the earliest known substitution cipher. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

5. Student should mention that “one-time pad” is an encryption scheme that is using a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then it should be discarded. Thus, each new message requires a new key of the same length as the new message. One-time pad scheme produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, it is mathematically provable that there is simply no way to break the cipher.

EXAM questions for the course TTM4135 - Information Security
June 2010

Part 2

This part consists of 40 questions. For every question 5 alternative answers are given, of which ONLY ONE is correct. If you chose the correct answer you will earn 1.8 points, otherwise you will loose 0.45 points (i.e. the penalty is -0.45 points). If you not choose any answer - then you will not get any points (i.e. the earned points are 0). Maximal number of points in this part of the exam is 72. Time for work on this test: ~120 minutes.

1. In X.800, **non-repudiation** is:
   a. assurance that data received is as sent by an authorized entity
   b. protection against denial by one of the parties in a communication
   c. assurance that the communicating entity is the one claimed
   d. prevention of the unauthorized use of a resource
   e. protection of data from unauthorized disclosure

2. Which one **IS NOT** a security mechanism in X.800:
   a. encipherment
   b. digital signatures
   c. data integrity
   d. Peer entity authentication
   e. traffic padding

3. What is **"Symmetric encryption"**:
   a. A mathematical procedure that is using a symmetric group.
   b. A form of cryptosystem that is based on groups of symmetry.
   c. A form of cryptosystem in which encryption and decryption are symmetric according to the ***y***-axis.
   d. A form of cryptosystem in which encryption and decryption are symmetric according to the ***x***-axis.
   e. A form of cryptosystem in which encryption and decryption are performed using the same key.

4. What is true for Steganography?
   a. Steganography is an old encryption technique.
   b. Steganography hides the very existence of a message by some means.
   c. Steganography is used in rotor machines.
   d. Steganography is a technique for message authentication.
   e. Steganography is used in public-key schemes.

5. Which two types of attacks on DES are slightly better than brute-force key search?
    a. Factorization of numbers and Discrete logarithm
    b. Statistical cryptanalysis and Testing of randomness
    c. Differential cryptanalysis and Linear cryptanalysis
    d. Man-in-the-middle and meet-in-the-middle attacks
    e. General Number sieve and Polynomial Quantum Factorization

6. The Shannon principle of “diffusion”
    a. makes relationship between ciphertext and key as complex as possible
    b. diffuses the plaintext among huge subset of plaintexts
    c. dissipates statistical structure of plaintext over bulk of ciphertext.
    d. diffuses the key and the plaintext among a subset of plaintexts
    e. makes the relationship between ciphertext and plaintext very complex

7. How many rounds has DES?
    a. 10
    b. 12
    c. 14
    d. 16
    e. 32

8. LUCIFER was the predecessor of DES and had the key length of:
    a. 64 bits
    b. 128 bits
    c. 56 bits
    d. 256 bits
    e. 96 bits

9. If (G,*) is a group then
    a. G is finite
    b. for every $x, y, z \in G$, $x+(y*z) = (x+y)*(x+z)$
    c. for every $x, y, z \in G$, $x*(y+z) = (x*y)+(x*z)$
    d. for every $x, y \in G$, $x*y = y*x$
    e. for every $x, y, z \in G$, $x*(y*z) = (x*y)*z$

10. gcd(19203, 62922)=
    a. 1
    b. 3
    c. 6
    d. 9
    e. 12

11. What is the correct hierarchy order of these algebraic structures (from lower to bigger number of axioms)
    a. ring → group → field
    b. field → ring → group
    c. field → group → ring
    d. group → field → ring
    e. group → ring → field

12. The nonlinear part of AES (the S-box) is performing computations in the following finite field:
    a. $GF(2^4)$
    b. $GF(2^8)$
    c. $GF(2^{16})$
    d. $GF(2^{32})$
    e. $GF(2^{33})$

13. The irreducible polynomial used in AES is:
    a. $m(x) = x^4 + x^3 + x + 1$
    b. $m(x) = x^{16} + x^5 + x^3 + x + 1$
    c. $m(x) = x^8 + x^4 + x^3 + x + 1$
    d. $m(x) = x^6 + x^3 + x + 1$
    e. $m(x) = x^6 + x^4 + x^2 + x + 1$

14. If $E_K(P)$ denotes an encryption of the plaintext block P with the key K by the block cipher E, then the cipher Output FeedBack (OFB) mode of operation can be described with the following equations:
    a. $C_i = E_K(C_{i-1} \text{ XOR } P_i \text{ XOR } O_i)$, $O_i = C_i$, $C_{-1} = IV$
    b. $C_i = P_i \text{ XOR } O_i$, $O_i = E_K(O_{i-1})$, $O_{-1} = IV$
    c. $C_i = E_K(P_i)$, $O_i = E_K(O_{i-1})$
    d. $C_i = C_{i-1} \text{ XOR } E_K(P_i)$, $C_{-1} = IV$
    e. $C_i = P_i \text{ XOR } E_K(i)$

15. Which attack is very efficient against Double-DES?

    a. meet-in-the-middle
    b. man-in-the-middle
    c. Linear cryptanalysis
    d. Differential cryptanalysis
    e. Statistical cryptanalysis

16. What is “Link encryption”?

    a. An encryption concept where the encryption function is performed at a low level of the communications hierarchy i.e. either at the physical or link layers.
    b. An encryption concept that guarantees the security of web data and web links.
    c. An encryption concept where the encryption function is performed at the application layer with specifically defined links.
    d. An encryption concept that puts the encryption at the application layer for all possible links.
    e. An encryption concept that encrypts the data traffic between different applications.

17. Which one of these numbers is prime?

    a. `2009`
    b. `2011`
    c. `2013`
    d. `2019`
    e. `2023`

18. The Fermat’s Little Theorem is

    a. The number of positive integers less than *n* and relatively prime to *n* is prime.
    b. $x^n + y^n = z^n$, has no solutions in natural numbers, for $n>2$.
    c. $a^b = b^a$, where a and b are prime numbers.
    d. $a^{p-1} = 1$ (mod p), where p is a prime number and GCD(a, p) = 1.
    e. The number of integers less than *n* that are divisors of *n* is composite.

19. Who are the authors of the first public-key algorithm

a. Diffie and Hellman

b. Rivest, Shamir, and Adleman

c. Daemen and Rijmen

d. IBM designers of DES

e. Miller and Rabin

20. On which hard mathematical problem, public-key algorithms based on elliptic curves rely their security?

a. Factorization of big numbers is hard

b. Solving multivariate quadratic equations is hard

c. Solving a SAT problem is hard

d. Computing discrete logarithms is hard

e. Solving the knapsack problem is hard

21. What are the ingredients of the **"RSA"** scheme:

a.

- p – prime number, (private, chosen)
- $n = p^2$, (public, calculated)
- e, with $\gcd(\Phi(n), e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
- $d = e^{-1}(\mathrm{mod}\ \Phi(n))$, (private, calculated)

b.

- p, q – two prime numbers, (public, chosen)
- $n = p\,q$, (private, calculated)
- e, with $\gcd(\Phi(n), e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
- $d = e^{-1}(\mathrm{mod}\ \Phi(n))$, (private, calculated)

c.

- p, q – two prime numbers, (private, chosen)
- $n = p\,q$, (public, calculated)
- e, with $\gcd(\Phi(n), e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
- $d = e^{-1}(\mathrm{mod}\ \Phi(n))$, (private, calculated)

d.

- p, q – two prime numbers, (private, chosen)
- $n = p\,q$, (public, calculated)
- e, (public, chosen)
- $d = e^{-1}(\mathrm{mod}\ \Phi(n))$, (private, calculated)

e.

- p, q – two prime numbers, (private, chosen)
- $n = p\,q$, (public, calculated)
- e, with gcd(n, e) = 1, $1 < e < n$, (public, chosen)
- $d = e^{-1}(\text{mod } n)$, (private, calculated)

22. Let (PU_a, PR_a) are the public and private key of Alice, and (PU_b, PR_b) are the public and private key of Bob. Let H() be a hash function, E(Key, Data) denote an encryption, and D(Key, Data) decryption operation, || denote a concatenation and Doc be a document. The digital signature algorithm performed by Alice, on the document Doc can be described as:
    a. Send: Doc || E(PU_a, H(Doc))
    b. Send: Doc || E(PU_b, H(Doc))
    c. Send: Doc || D(PR_b, H(Doc))
    d. Send: Doc || D(PR_a, H(Doc))
    e. Send: Doc || E(PR_b, H(Doc))

23. Chinese Reminder Theorem is used in RSA in order
    a. To compute the private exponent d.
    b. To find strong prime numbers.
    c. To speed up the decryption with the private key approximately 4 times.
    d. To speed up the verification process.
    e. To speed up the encryption with the public key approximately 4 times.

24. The attack that is exploiting the variations in operations that depend on different 0s and 1s in the private key are called
    a. linear attack
    b. differential attack
    c. exponentiation attack
    d. timing attack
    e. man-in-the-middle attack

25. Diffie-Helman algorithm is used for
    a. digital signature
    b. encryption
    c. decryption
    d. key exchange
    e. authentication

26. An ECC (Elliptic Curve Cryptography) scheme with size of 256 bits has an equivalent security of a symmetric scheme with
    a. 128 bits
    b. 256 bits
    c. 512 bits
    d. 1024 bits
    e. 3072 bits

27. Let C(Key, M) denote a message authentication code function, produced for the message M and a shared key Key. Let E(Key, M) denote encryption of a message M with a key Key, and let || denote the concatenation. If Alice send to Bob the following information: E(K2, M) || C(K1, E(K2, M)) where K1 and K2 are shared secret keys, then it is

    a. just a message authentication
    b. message authentication and confidentiality where authentication is tied to the plaintext
    c. message authentication and confidentiality where authentication is tied to the ciphertext
    d. just a message confidentiality
    e. message authentication and confidentiality where authentication is tied both to the plaintext and to the ciphertext

28. If we have a hash function with a digest size of n bits, with the birthday paradox attack approximately how much hash operations we need in order to find a collision

    a. $2^{n/2}$
    b. 2n
    c. 2^{n}
    d. 2^{n-1}
    e. n^{n}

29. The word size of SHA-512 is
    a. 16 bits
    b. 32 bits
    c. 64 bits
    d. 128 bits
    e. 512 bits

30. The Whirlpool hash function is based on

a. MD5 design
b. SHA-1 design
c. DES design
d. AES design
e. Blowfish design

31. If we perform the following operations:

$$\text{Hash}[(K^{+} \text{ XOR opad}) \,||\, \text{Hash}[(K^{+} \text{ XOR ipad})||M)]]$$

where K^{+} is a properly padded secret key, opad and ipad are specific padding constants, and M is a message, then we have performed:

a. 2-Hash operation
b. Double-Hash operation
c. NMAC operation
d. CMAC operation
e. HMAC operation

32. How many steps has Needham-Schroeder Protocol?

a. 3
b. 4
c. 5
d. 6
e. 7

33. How big is the digital signature produced with DSA?

a. 160 bits
b. 256 bits
c. 320 bits
d. 512 bits
e. 1024 bits

34. Kerberos is:

a. A part of PKI.
b. A part of X.509 public-key infrastructure.
c. A pubic-key based key distribution center
d. A symmetric key based encryption center
e. An authentication service designed for use in a distributed environment.

35. Which MAC is used in S/MIME?
    a. CMAC with SHA-2
    b. NMAC with SHA-1
    c. HMAC with MD4
    d. HMAC with MD5
    e. HMAC with SHA-1

36. Which three functional areas are provided by IPSec?
    a. Authentication, Confidentiality, and Key management
    b. Authentication, Error detection, and Error correction
    c. Authentication, Key generation, and Certificate exchange
    d. Encryption, Decryption, and Certificate validation
    e. Authentication, Confidentiality, and Digital Signatures

37. What algorithm is used for message authentication in TLS
    a. AES-OFB
    b. AES-CBC
    c. NMAC
    d. HMAC
    e. CMAC

38. What is a **"Clandestine user"**?
    a. An individual who is not authorized to use computer and who penetrates a system's access controls to exploit a legitimate user's account.
    b. An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.
    c. A legitimate user who accesses data, programs or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
    d. An individual who is authorized to use computer as supervisor but who penetrates into other legitimate user's account.
    e. An insider hacker who is authorized to use computers.

39. In Information Security a **"Logic Bomb"** refers to a malicious code that:
    a. propagates copies of itself to other computers.
    b. triggers action when a specific condition occurs.
    c. contains unexpected additional functionality.
    d. allows unauthorized access to functionality.
    e. sends large volumes of unwanted e-mail.

40. The **“packet-filtering router”** is:

a. not a part of a dual-homed bastion host

b. not a part of a single-homed bastion host

c. a type of firewall

d. a circuit-level gateway firewall

e. an application-level gateway firewall

KEY for Part 2

1. b,
2. d,
3. e,
4. b,
5. c,
6. c,
7. d,
8. b,
9. e,
10. b,
11. e,
12. b,
13. c,
14. b,
15. a,
16. a,
17. b,
18. d,
19. a,
20. d,
21. c,
22. d,
23. c,
24. d,
25. d,
26. a,
27. c,
28. a,
29. c,
30. d,
31. e,
32. c,
33. c,
34. e,
35. e,
36. a,
37. d,
38. b,
39. b,
40. c