**EXAM questions for the course TTM4135 - Information Security**

**June 2011**

**Part 1**

*This part consists of 5 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: Public key cryptography

1. (4 points) What is “Asymmetric encryption”?
2. (4 points) On which premise relies the strength of RSA?
3. (6 points) What is “Digital Certificate”?
4. (7 points) What is “Public Key Infrastructure”?
5. (7 points) What is OAEP?

**KEY for Part 1**

1. Student should mention that the asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using two different keys called a public key and a private key.
2. Student should mention that the strength of RSA rely on the hardness of factoring big numbers.
3. Student should mention that “Digital Certificate” is a digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key.
4. Student should mention that the “Public Key Infrastructure” is a set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public - private key pairs, including the ability to issue, maintain, and revoke public key certificates.
5. Student should mention that OAEP is the recommended way of use of RSA algorithm that is resistant to CCA attacks.

**EXAM questions for the course TTM4135 - Information Security**

**June 2011**

**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.*

Multiple choice answers Candidate nr \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**USE CAPITAL LETTERS!**

**PLEASE FILL IN AND DELIVER THIS PAGE**

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

1. What is a common technique for masking contents of messages or other information traffic so that opponents cannot extract the information from the message?
   1. integrity
   2. analysis
   3. masquerade
   4. encryption
   5. authentication
2. When an attacker performs a capture of a data unit and its subsequent retransmission to produce an unauthorized effect, which attack he is performing?
   1. Disruption
   2. Replay
   3. Masquerade
   4. Service denial
   5. Unauthorized change of the content
3. If both sender and receiver use the same key, the system is referred to as:
   1. symmetric key encryption
   2. asymmetric key encryption
   3. public key encryption
   4. one key encryption
   5. same key encryption
4. A way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is:
   1. polyalphabetic substitution cipher
   2. cryptanalysis
   3. polyanalysis cipher
   4. rail fence cipher
   5. multiple cipher
5. What is the block cipher structure in DES?
   1. SAC
   2. Shannon
   3. Feistel
   4. Rendell
   5. One Way Permutation
6. Which cryptanalysis attack was the first published attack that is capable of breaking DES in about 247 encryptions.
   1. Meet-in-the-middle
   2. Linear
   3. Differential
   4. Statistical
   5. Confusion
7. The greatest common divisor of two integers is the largest positive integer that exactly \_\_\_\_\_\_\_\_\_ both integers.
8. squares
9. multiplies
10. exponentially multiplies
11. add
12. divides
13. A group (G, \*) is said to be \_\_\_\_\_\_\_\_\_ if it satisfies the condition a \* b = b \* a for all a, b in G.
    1. cyclic
    2. abelian
    3. associative
    4. distributive
    5. swappable
14. Over which finite field in AES, the S-box operations are performed?
    1. GF(24)
    2. Z17
    3. GF(28)
    4. GF(232)
    5. Z257
15. How many stages have the final round of both encryption and decryption in AES?
    1. one
    2. two
    3. three
    4. four
    5. five
16. The main reason why Triple-DES was not kept as the only standard for block ciphers and have been replaced by AES is that
    1. it has too short key
    2. it has too long key
    3. it is patented
    4. it is old
    5. it is slow
17. What is the term used for the secret key for symmetric encryption that is generated for use for a short period of time?
    1. stream key
    2. session key
    3. strategic key
    4. sequence key
    5. master key
18. The distribution of bits in a random number sequence should be \_\_\_\_\_\_\_\_\_\_\_ , therefore the frequency of occurrence of ones and zeros should be approximately equal.
19. reversed
20. streamed
21. uniform
22. independent
23. random
24. If *p* is prime and *a* is a positive integer, then *ap* = *a* mod *p* is an alternative form of which theorem?
    1. Miller's
    2. Euler's
    3. Fermat's
    4. Newton's
    5. Shannon’s
25. Which algorithm is typically used to test a large number for primality?
    1. Fermat
    2. Euler
    3. Miller–Rabin
    4. Newton
    5. RSA
26. The RC4 stream cipher is:
    1. bit oriented
    2. 16 bit oriented
    3. Big-endian oriented
    4. Little-endian oriented
    5. byte oriented
27. The key exchange protocol is vulnerable to a \_\_\_\_\_\_\_\_\_\_ attack because it does not authenticate the participants.
28. chosen ciphertext
29. man - in - the - middle
30. side channel
31. replay
32. differential cryptanalysis
33. If three points on an elliptic curve lie on a straight line their sum is \_\_\_\_\_\_\_\_\_\_ .
    1. undetermined
    2. infinite
    3. -1
    4. 1
    5. 0
34. SHA-1 produces a hash value of \_\_\_\_\_\_\_\_\_\_ bits.
    1. 64
    2. 128
    3. 160
    4. 256
    5. 512
35. What does it mean that a function H is “**collision resistant**”?
    1. It can be applied to any sized message *M*
    2. It is easy to compute *h* = H(*M*) for any message *M*
    3. Given *h*, it is infeasible to find *x* s.t. H(*x*) = *h*
    4. Given *x*, it is infeasible to find *y* s.t. H(*y*) = H(*x*)
    5. It is infeasible to find any *x*, *y* s.t. H(*y*) = H(*x*)
36. Insertion of messages into the network from a fraudulent source is a \_\_\_\_\_\_\_\_\_\_ attack.
    1. masquerade
    2. source repudiation
    3. sequence modification
    4. spoofing
    5. denial of service
37. What is CMAC?
    1. MAC based on CFB mode
    2. MAC based on CTR mode
    3. MAC based on CCT mode
    4. MAC based on OFB mode
    5. MAC based on CBC mode
38. DSS is a \_\_\_\_\_\_\_\_\_\_ technique.
    1. public key
    2. firewall
    3. timestamp
    4. private key
    5. antivirus
39. When a user is computing the hash of a message and then encrypting the hash with his private key, he is producing:
    1. a hash code
    2. a timestamp
    3. a message digest
    4. a digital signature
    5. a session key
40. Key distribution often involves the use of \_\_\_\_\_\_\_\_\_ which are generated and distributed for temporary use between two parties.
    1. session keys
    2. private key certificates
    3. public key certificates
    4. master keys
    5. public keys
41. Which infrastructure has the principal objective to enable secure, convenient and efficient acquisition of public keys.
    1. PKI
    2. KDC
    3. CRL
    4. IETF
    5. Kerberos
42. The set of managed nodes that share the same Kerberos database is called:
    1. A Kerberos realm
    2. A Kerberos network
    3. Kerberos tickets
    4. A Kerberos area
    5. A Kerberos universe
43. Presenting an identifier to the security system is the \_\_\_\_\_\_\_\_\_\_ step.
    1. identification
    2. verification
    3. authentication
    4. clarification
    5. non-repudiation
44. WAP security is primarily provided by the \_\_\_\_\_\_\_\_\_\_ which provides security services between the mobile device and the WAP gateway to the Internet.
    1. MSDU
    2. TKIP
    3. CCMP
    4. WTLS
    5. Wi-Fi
45. The term used for certified 802.11b products is \_\_\_\_\_\_\_\_\_\_\_ .
    1. WAP
    2. WEP
    3. Wi-Fi
    4. WPA
    5. Zig-bee
46. PGP provides authentication through the use of \_\_\_\_\_\_\_\_\_ .
    1. radix - 64
    2. digital signatures
    3. asymmetric block encryption
    4. symmetric block encryption
    5. data compression
47. Which hash functions are used in S/MIME?
    1. MD5 and SHA-1
    2. MD4 and MD5
    3. MD5 and SHA-2
    4. SHA-1 and SHA-2
    5. MD4, MD5, SHA-1 and SHA-2
48. Authentication applied to the entire original IP packet is \_\_\_\_\_\_\_\_\_ .
    1. security mode
    2. tunnel mode
    3. transport mode
    4. cipher mode
    5. application mode
49. Authentication applied to all of the packet except for the IP header is \_\_\_\_\_\_\_\_\_ .
    1. security mode
    2. tunnel mode
    3. transport mode
    4. cipher mode
    5. application mode
50. 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 is called:
    1. Clandestine User
    2. Masquerader
    3. Emissary
    4. Misfeasor
    5. Sniffer
51. A technique that focuses on characterizing the past behaviour of individual users or related groups of users and then detecting significant deviations is called:
    1. Statistical anomaly
    2. Profile - based anomaly
    3. Threshold
    4. Action condition
    5. Markov chain
52. A secret entry point into a program that allows someone who is aware of it to gain access without going through the usual security access procedures is called:
    1. secret password
    2. payback entry
    3. Trojan horse
    4. logic entry
    5. backdoor
53. Which attacks make computer systems inaccessible by flooding servers, networks, or even end user systems with useless traffic so that legitimate users can no longer gain access to those resources?
    1. Blacklisting attacks
    2. PWC
    3. DDoS
    4. Flooding attacks
    5. Spoofing attacks

1. \_\_\_\_\_\_\_\_\_ can be effective means of protecting a local system or network of systems from network based security threats while at the same time affording access to the outside world via wide area networks and the Internet.
   1. VPNs
   2. SOCKS
   3. Firewalls
   4. Proxys
   5. Antivirus packakges
2. Which firewall concept applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
   1. packet filtering
   2. distributed
   3. stateful inspection
   4. host – based
   5. demilitarized zone

**KEY for Part 2**

1. D
2. B
3. A
4. A
5. C
6. C
7. E
8. B
9. C
10. C
11. E
12. B
13. C
14. C
15. C
16. E
17. B
18. E
19. C
20. E
21. A
22. E
23. A
24. D
25. A
26. A
27. A
28. A
29. D
30. C
31. B
32. A
33. B
34. C
35. D
36. B
37. E
38. C
39. C
40. A