Computer Security (Evaluation, Part I - Crypto)

this is a randomly generated examen subject, current time: 1/17/2019 6:56:09 PM typeset in LaTeX

1. **What is the Euler ϕ function of integer n=119**

a) 98
b) 97
c) 99
d) 96

2. **Let n = 55 which of the following exponent cannot be used for RSA:**

a) 5
b) 3
c) 2
d) 7

3. **The Cesar cipher resembles:**

a) a block cipher
b) a mono-alphabetic substitution
c) a rotor machine
d) a stream cipher

4. **Which of the following equations describes the Feistel network :**

a) $L_i = R_i, R_i = L_i \oplus f_i(R_i)$
b) $L_i = L_{i-1} \oplus f_i(R_{i-1}), R_i = R_{i-1}$
c) $L_i = L_i \oplus f_i(R_i), R_i = R_i$
d) $L_i = f(R_{i-1}), R_i = L_{i-1} \oplus f_i(R_{i-1})$

5. **Consider the group formed by Z^*_{15} under multiplication. Which of the following is a generator:**

a) 3
b) 5
c) 15
d) Z^*_{15} doesn't have generators

6. **What is the Euler ϕ function of integer n= 77**

a) 30
b) 60
c) 50
d) 40

7. **What is the Euler ϕ function of integer n=100**

a) 30
b) 40
c) 20
d) 10

8. **Let c = 55 , n = 221 which of the following may be the encrypted message in case of Rabin encryption:**

a) 85
b) 86
c) 134
d) 87

9. **Which of the following is true about the one-time pad:**

a) it requires a key of the same length as the message
b) it is not secure to re-use a key
c) the message must be perfectly random
d) cannot be broken regardless of the computational power

10. **What can you say about $H(k||m)$ when put in place of a MAC:**

a) it is secure
b) it is insecure for general purposes
c) it is secure only if the message has fixed size
d) it is insecure if we know the message

11. **Concatenation attack were described during the lecture as:**

a) attack on the Feistel network, by which an adversary can decrypt
b) attacks on messages authentication codes, in particular the HMAC
c) concatenations of messages with key that result in insecure encryption schemes
d) attacks on the simple key-message concatenation for building a MAC

12. **What is the Euler ϕ function of integer n= 161**

a) 134
b) 132
c) 138
d) 136

13. **Which of the following hold about the AES:**

a) it's a block cipher
b) it's the standardized version of the Rijndael cipher designed by Belgian cryptographers Vincent Rijmen and Joan Daemen
c) it has keys of 128, 192 and 256 bits
d) it's a Feistel cipher

14. **Which of the following will produce a compile error in .NET, (consider SymmetricAlgorithm mySymmetricAlg;):**

a) mySymmetricAlg = new RSACryptoServiceProvider();
b) mySymmetricAlg = new DES();
c) mySymmetricAlg = new DESCryptoServiceProvider();
d) mySymmetricAlg = DES.Create();

15. **What is a random oracle?**

a) a padding scheme

b) an object that outputs random data to simulate hash functions

c) a Feistel network used for padding

d) an object that performs guesses to break cryptosystems

16. **What is the Euler ϕ function of integer n= 133**

a) 112

b) 110

c) 114

d) 108

17. **What is the Euler ϕ function of integer n=221**

a) 193

b) 192

c) 194

d) 196

18. **Let n = 115 and e =93 which is the private exponent d for RSA decryption:**

a) 53

b) 63

c) 33

d) 23

19. **Ignore the security level, which of the following public exponents will give the fastest signing time for RSA:**

a) the public exponent cannot guarantee signing time

b) 3

c) 5

d) 65537

20. **Consider a Feistel network having as input L=F0 and R =0F while the round function is logical AND with key K =FF. What is the output:**

a) L = 0F, R = EE

b) L = 0F, R = F0

c) L = 0F, R = EF

d) L = 0F, R = AA

21. **What is the Euler ϕ function of integer n=187**

a) 140

b) 120

c) 160

d) 110

22. **Let n=77 and m= 25, decryption of the message modulo p and q (to be merged by CRT) are:**

a) 4 and 3

b) not enough data to tell

c) 2 and 4

d) 4 and 5

23. **Which of the following is correct about the round function of a Feistel network:**

a) technically, it can be any function but the result is not necessarily a secure block-cipher

b) must be a one-way function

c) takes the right block as input

d) takes as input the round function

24. **Which of the following is correct regarding security notions for symmetric encryptions:**

a) SS ↔ IND

b) IND → RoR

c) RoR ↔ IND

d) RoR → IND

25. **Consider the one-time pad, plaintext is 0xffh şi and key is 0xff. Which of the following sentences are true:**

a) if captured by an adversay, the output can be broken and the plaintext recovered

b) key is incorrect as it must be random

c) output is 0xFF

d) output is 0x00

26. **What are the characteristics of counter-mode compared to CBC:**

a) encryption in counter-mode is deterministic

b) counter-mode is insecure

c) counter-mode allows decryption of the current block if the previous is lost

d) counter-mode allows encrypting the counter in advance

27. **Attack types on digital signatures include:**

a) total break
b) existential forgery
c) collective forgery
d) partial forgery

28. **In case of the Diffie-Hellman key-exchange, let g=2 (ignore if this is a generator or not), $p = 127$, $g^x = 32$ and $g^y = 4$ which is the common key:**

a) 64
b) 8
c) 32
d) 16

29. **For the BBS PRNG given the following parameters, which is the output x_1, x_2, x_3, $n = 13, x_0 = 2$:**

a) 2, 4, 8
b) 4, 3, 9
c) 4, 8, 16
d) 3, 7, 9

30. **Consider that the Enigma machine had 3 plugs that fit into 10 holes, what is the size of the key for Enigma? (ignore any other component)**

a) 25200
b) 18900
c) 3150
d) 65536

31. **If n =209 which of the following exponents can be used for RSA?**

a) 7
b) 5
c) 3
d) not enough data to tell, since it is unclear if we are talking about the private or public exponent

32. **For the BBS PRNG given the following parameters, which is the output x_1, x_2, x_3, $n = 11, x_0 = 3$:**

a) 3, 9, 13
b) 9, 4, 5
c) 5, 7, 9
d) 3, 9, 27

33. **If a hash function has an output on 32 de bits, for a given output we may expect to find an output after how many steps:**

a) 2^{32}
b) 2^{16}
c) 2^{31}
d) 2^{64}

34. **Consider the group formed by Z_6^* under multiplication. Which of the following is a generator:**

a) 1
b) 6
c) Z_6^* doesn't have generators
d) 5

35. **The Enigma machine resembles:**

a) a poly-alphabetic substitution
b) none of the above, this is just a historical artefact
c) a stream cipher
d) a block cipher

36. **Let n = 221 and exponent e =5 which is the exponent d for RSA decryption:**

a) 77
b) 66
c) 55
d) 5

Name: Year :

Date: Correct answers:

♠	a)	b)	c)	d)
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				
26				
27				
28				
29				
30				
31				
32				
33				
34				
35				
36				
37				
38				
39				
40				
41				
42				
43				
44				
45				
46				
47				
48				
49				
50				