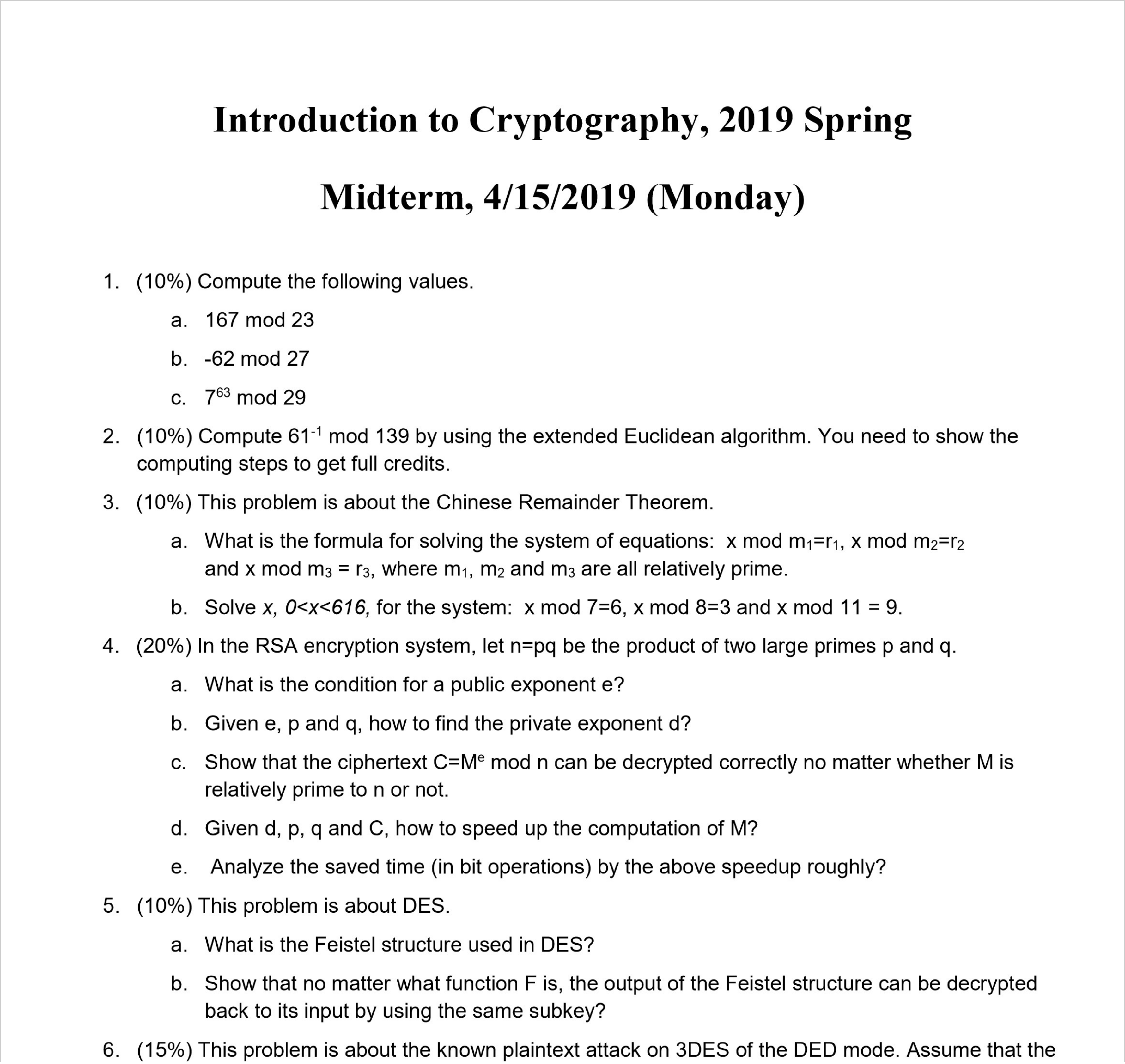
Midterm-Solutions

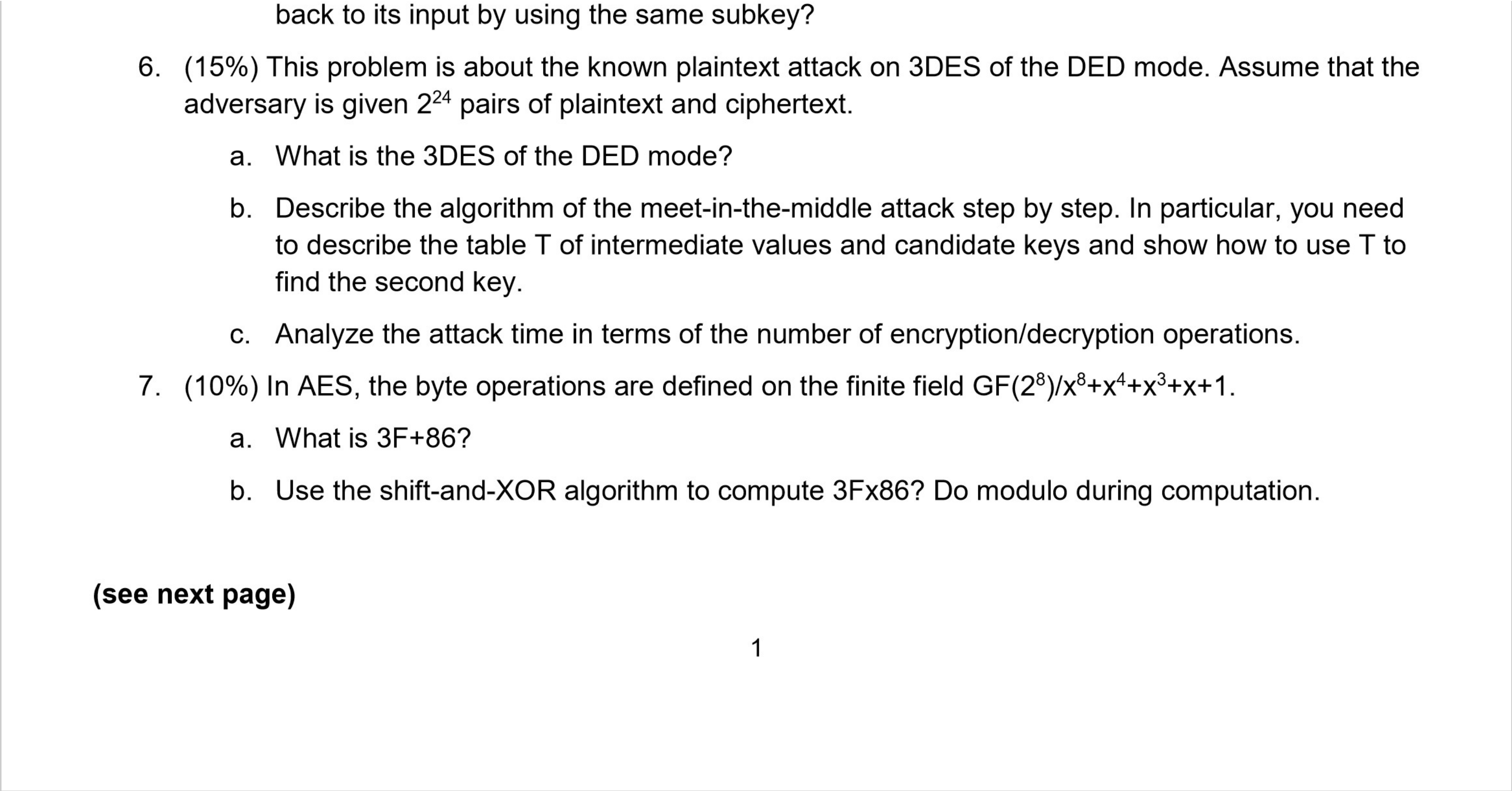
2019年4月15日　　上午 08:32



Introduction to Cryptography, 2019 Spring

Midterm, 4/15/2019 (Monday)

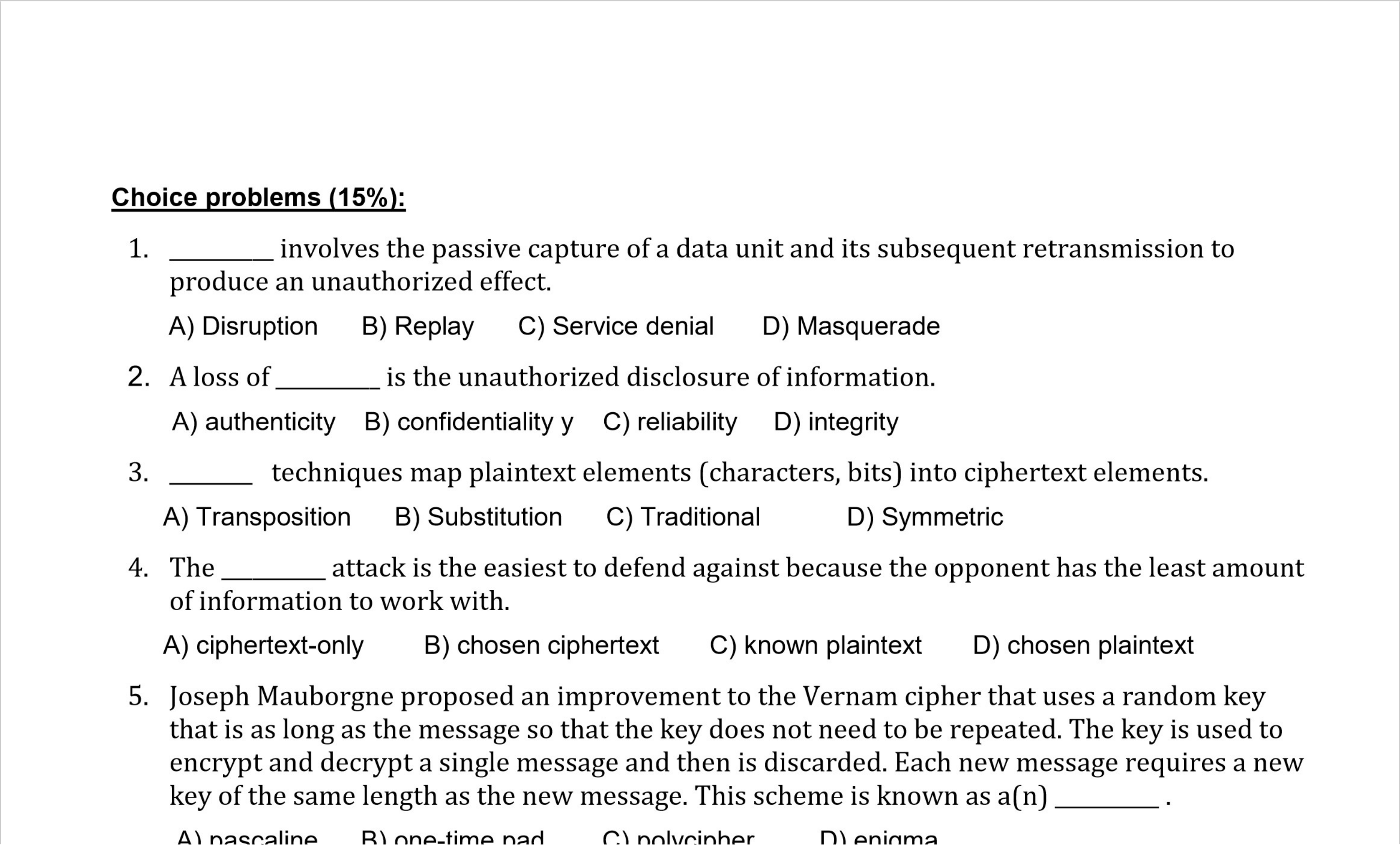
1. (10%) Compute the following values.
    a. 167 mod 23
    b. -62 mod 27
    c. 7^{63} mod 29
2. (10%) Compute 61^{-1} mod 139 by using the extended Euclidean algorithm. You need to show the computing steps to get full credits.
3. (10%) This problem is about the Chinese Remainder Theorem.
    a. What is the formula for solving the system of equations: x mod m_1=r_1, x mod m_2=r_2 and x mod m_3 = r_3, where m_1, m_2 and m_3 are all relatively prime.
    b. Solve *x, 0<x<616,* for the system: x mod 7=6, x mod 8=3 and x mod 11 = 9.
4. (20%) In the RSA encryption system, let n=pq be the product of two large primes p and q.
    a. What is the condition for a public exponent e?
    b. Given e, p and q, how to find the private exponent d?
    c. Show that the ciphertext C=M^e mod n can be decrypted correctly no matter whether M is relatively prime to n or not.
    d. Given d, p, q and C, how to speed up the computation of M?
    e. Analyze the saved time (in bit operations) by the above speedup roughly?
5. (10%) This problem is about DES.
    a. What is the Feistel structure used in DES?
    b. Show that no matter what function F is, the output of the Feistel structure can be decrypted back to its input by using the same subkey?
6. (15%) This problem is about the known plaintext attack on 3DES of the DED mode. Assume that the



back to its input by using the same subkey?

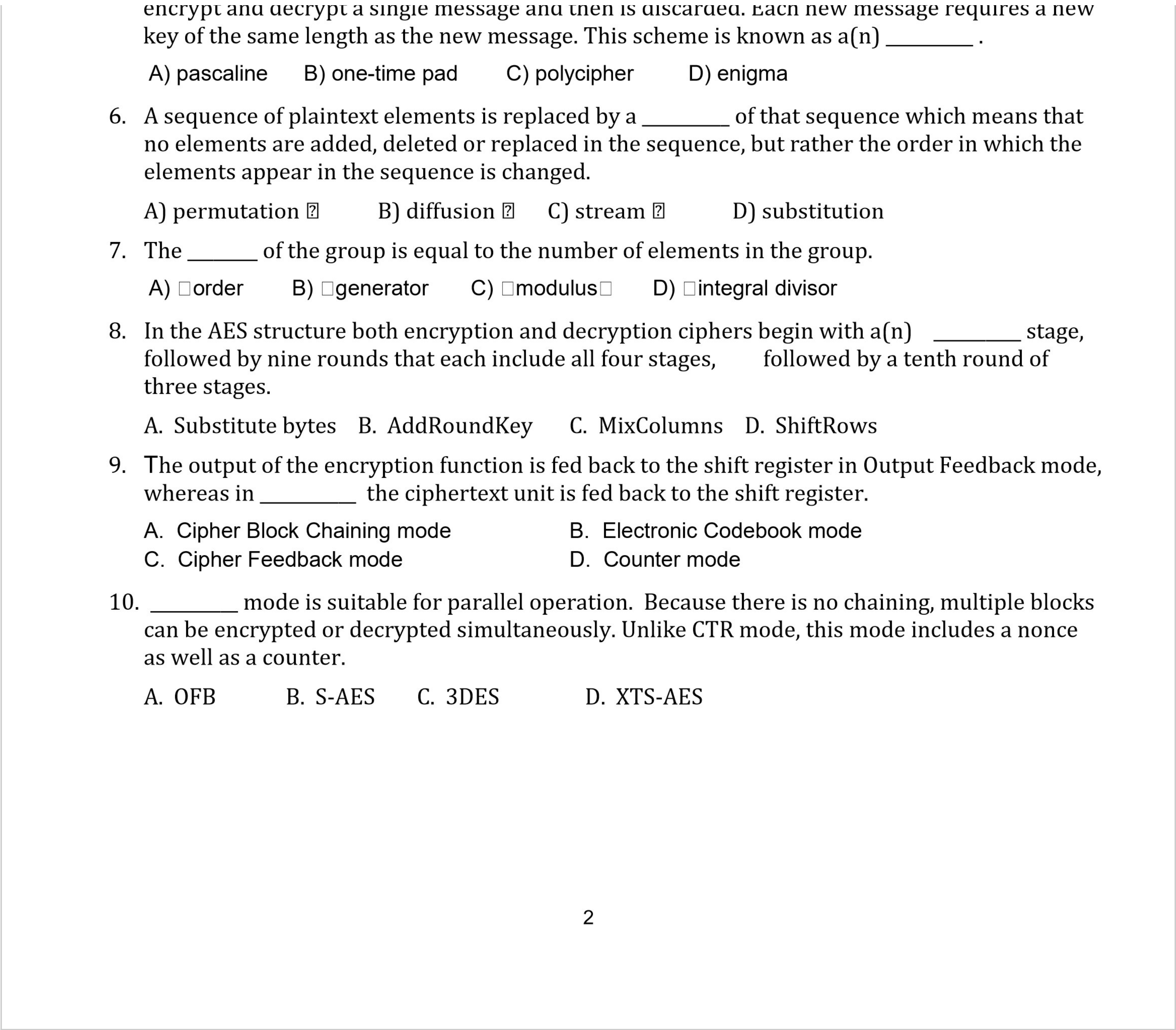
6. (15%) This problem is about the known plaintext attack on 3DES of the DED mode. Assume that the adversary is given 2^{24} pairs of plaintext and ciphertext.
   a. What is the 3DES of the DED mode?
   b. Describe the algorithm of the meet-in-the-middle attack step by step. In particular, you need to describe the table T of intermediate values and candidate keys and show how to use T to find the second key.
   c. Analyze the attack time in terms of the number of encryption/decryption operations.
7. (10%) In AES, the byte operations are defined on the finite field $GF(2^8)/x^8+x^4+x^3+x+1$.
   a. What is 3F+86?
   b. Use the shift-and-XOR algorithm to compute 3Fx86? Do modulo during computation.

(see next page)



Choice problems (15%):

1. ________ involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
   A) Disruption B) Replay C) Service denial D) Masquerade
2. A loss of ________ is the unauthorized disclosure of information.
   A) authenticity B) confidentiality y C) reliability D) integrity
3. ______ techniques map plaintext elements (characters, bits) into ciphertext elements.
   A) Transposition B) Substitution C) Traditional D) Symmetric
4. The ________ attack is the easiest to defend against because the opponent has the least amount of information to work with.
   A) ciphertext-only B) chosen ciphertext C) known plaintext D) chosen plaintext
5. Joseph Mauborgne proposed an improvement to the Vernam cipher that uses a random key that is as long as the message so that the key does not need to be repeated. The key is used to encrypt and decrypt a single message and then is discarded. Each new message requires a new key of the same length as the new message. This scheme is known as a(n) ________ .
   A) pascaline B) one-time pad C) polycipher D) enigma



encrypt and decrypt a single message and then is discarded. Each new message requires a new key of the same length as the new message. This scheme is known as a(n) _________ .

A) pascaline B) one-time pad C) polycipher D) enigma

6. A sequence of plaintext elements is replaced by a _________ of that sequence which means that no elements are added, deleted or replaced in the sequence, but rather the order in which the elements appear in the sequence is changed.

A) permutation ⍰ B) diffusion ⍰ C) stream ⍰ D) substitution

7. The _______ of the group is equal to the number of elements in the group.

A) □order B) □generator C) □modulus□ D) □integral divisor

8. In the AES structure both encryption and decryption ciphers begin with a(n) _________ stage, followed by nine rounds that each include all four stages, followed by a tenth round of three stages.

A. Substitute bytes B. AddRoundKey C. MixColumns D. ShiftRows

9. The output of the encryption function is fed back to the shift register in Output Feedback mode, whereas in __________ the ciphertext unit is fed back to the shift register.

A. Cipher Block Chaining mode B. Electronic Codebook mode
C. Cipher Feedback mode D. Counter mode

10. _________ mode is suitable for parallel operation. Because there is no chaining, multiple blocks can be encrypted or decrypted simultaneously. Unlike CTR mode, this mode includes a nonce as well as a counter.

A. OFB B. S-AES C. 3DES D. XTS-AES

Solutions:

2019年4月15日 上午 08:54

1. (a) 6

(b) 19

(c) $7^{63} \bmod 29 = 7^{63 \bmod 28} \bmod 29 = 7^7 \bmod 29$

$= 49^3 \cdot 7 \bmod 29 = 20 \cdot 20 \cdot 20 \cdot 7 \bmod 29$

$= 1$

2

$$\begin{aligned}
0 \cdot 61 + 1 \cdot 139 &= 139 \\
1 \cdot 61 + 0 \cdot 139 &= 61 && \big\uparrow x{-2} \\
-2\ 61 + 1 \cdot 139 &= 17 && \big\uparrow x{-3} \\
7 \cdot 61 + -3 \cdot 139 &= 10 && \big\uparrow x{-1} \\
-9 \cdot 61 + 4 \cdot 139 &= 7 && \big\uparrow x{-1} \\
16 \cdot 61 + (-7) \cdot 139 &= 3 && \big\uparrow x \cdot 2 \\
-41 \cdot 61 + 18 \cdot 139 &= 1
\end{aligned}$$

$\Rightarrow 61^{-1} \bmod 139 = -41 \bmod 139 = 98$

3 (a) $x = \left[r_1 \left(m_2 m_3 \cdot (m_2 m_3)^{-1} \bmod m_1 \right) \right.$

$+ r_2 \left(m_1 m_3 \cdot (m_1 m_3)^{-1} \bmod m_2 \right)$

$\left. + r_3 \left(m_1 m_2 \ (m_1 m_2)^{-1} \bmod m_3 \right) \right] \bmod m_1 m_2 m_3$

(b) $x = [6 \cdot 88 \cdot 88^{-1} \bmod 7 + 3 \cdot 77 \cdot 77^{-1} \bmod 8 + 9 \cdot 56 \cdot 56^{-1} \bmod 11] \bmod 616$

$= [6 \cdot 88 \cdot 2 + 3 \cdot 77 \cdot 5 + 9 \cdot 56 \cdot 1] \bmod 616$

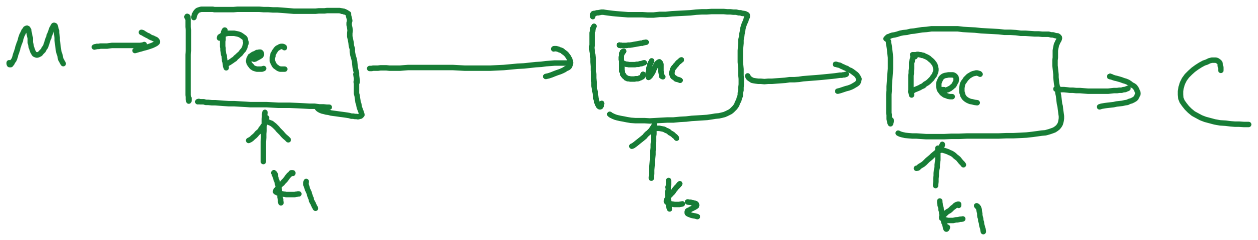
$= 251$

4. See the course slides

5. See the course slides

6. See the course slides.

Note that DED-3DES is



7 (a) 10111001 = B9

7 (a) 1011 1001 = B9

(b) G = 3F = 0011 1111

$b = b_7\, b_6\, b_5\, b_4\, b_3\, b_2\, b_1\, b_0 = 86 = 1000\ 0110$

$g(x) = x^8 + x^4 + x^3 + x + 1 = 1\ 0001\ 1011$

We use table: f = 0000 0000 intial

XOR g(x) if the leading bit is 1

	i	f (shift-XOR)	f (mod g(x))
1	7	0011 1111	0011 1111
0	6	0111 1110	0111 1110
0	5	1111 1100	1111 1100
0	4	1 1111 1000	1110 0011
0	3	1 1100 0110	1101 1101
1	2	1 1000 0101	1001 1110
1	1	1 0000 0011	0001 1000
0	0	0011 0000	$\underline{0011\ 0000}$

$\downarrow$ 30 HEX

Choice Problems

1. B
2. B

3	B
4.	A
5.	B
6.	A
7.	A
8.	B
9	C
10	D