1. Among the following ciphers, which is strongest? D

单选题 (6 分) 6 分

○ A.

DES

○ B.

3DES

○ C.

Caesar cipher

○ D.

AES

3.

The purpose of is to determine whom you are talking to before revealing sensitive information or entering into a business deal B

单选题 (6 分) 6 分

○ A.

integrity control 完整性控制

○ B.

Authentication 认证

○ C.

Secrecy 保密

○ D.

Nonrepudiation

4.

Which is incorrect？ A

单选题 (6 分) 6 分

○ A.

it would be more secure if the encryption and decryption algorithms are kept secret 加密算法和解密算法应该都要公开

○ B.

all encrypted messages must contain some redundancy

所有加密邮件必须包含一些冗余

○ C.

some measure must be taken to prevent active intruders from playing back old messages

○ D.

to achieve security, the cryptographer should make sure that the system is unbreakable even if his opponent can encrypt arbitrary amounts of chosen plaintext
为了实现安全性，密码学家应确保系统牢不可破，即使他的对手可以加密任意数量的选定明文。

Encrypt 加密 decrypt 是解密

5.

Among the following ciphers, ________ is unbreakable. D
单选题 (6 分) 6 分

○ A.

AES

○ B.

DES

○ C.

RSA

○ D.

one-time-pad encryption（单次密钥）

2. 6.

Cipher block chaining can be used to prevent attack to ________ . B
单选题 (6 分) 6 分

○ A.

RSA

○ B. 密码块链接（Cipher Block Chaining，CBC）可以用来防止对 AES 进行攻击，这是因为 CBC 可以增强 AES 的安全性。

AES

○ C.

SHA-1

○ D.

PGP

3. 7.

The two way challenge response protocol for authentication can be defeated by ____ D

单选题 (6 分) 6 分

1. ○ A.

man in the middle attack

2. ○ B.

bucket brigade attack

3. ○ C.

replay attack

4. ○ D.

reflection attack

Which key is the browser used to verify the certificate of the website?

单选题 (6 分) 6 分 A

5. ○ A.

The public key of the CA

6. ○ B.

The public key of the website

7. ○ C.

The private key of the website

8. ○ D.

The private key of the browser

4. 9.

Which key is used to verify the certificate? A

单选题 (6 分) 6 分

1. ○ A.

The public key of the CA who signed the certificate

2. ○ B.

The private key of the CA who signed the certificate

3. ○ C.

The private key of the user who own the certificate

4. ○ D.

The public key of the user who own the certificate

5. 10.

Which sentence is not correct? B
单选题 (6 分) 6 分

1. ○ A.

One of cryptographic principles is redundancy, another is freshness.

2. ○ B.

The replay attack is a way to authenticate by tricking the target into providing the answer to its own challenge. 重放攻击可以通过复制并重新发送已认证的请求来获得授权，但它不是通过欺骗目标让其提供自己的挑战答案来认证的

3. ○ C.

Diffie-Hellman key exchange algorithm allows strangers to establish a shared secret key but has problem of man-in-the-middle attack.

4. ○ D.

Quantum cryptography is one of method to transmit one-time pad over network but the equipment is complex and expensive now.

6. 11.

Which key is used to decrypt data when using public-key cryptography? C
单选题 (6 分) 6 分

1. ○ A.

The sender’s private key

2. ○ B.

The receiver’s public key

3. ○ C.

The receiver’s private key

4. ○ D.

The sender’s public key

7. 12.

The main public-key algorithm is ____________________ which derives its strength from the fact that it is very difficult to factor large numbers. A. B. C. D. (很难分解大数字) D

单选题 (6 分) 6 分

1. ○ A.

MD5

2. ○ B.

AES

3. ○ C.

DES

4. ○ D.

RSA

The firewall is based on ________.

单选题 (10 分) 10 分

1. ● A.

access control

2. ○ B.

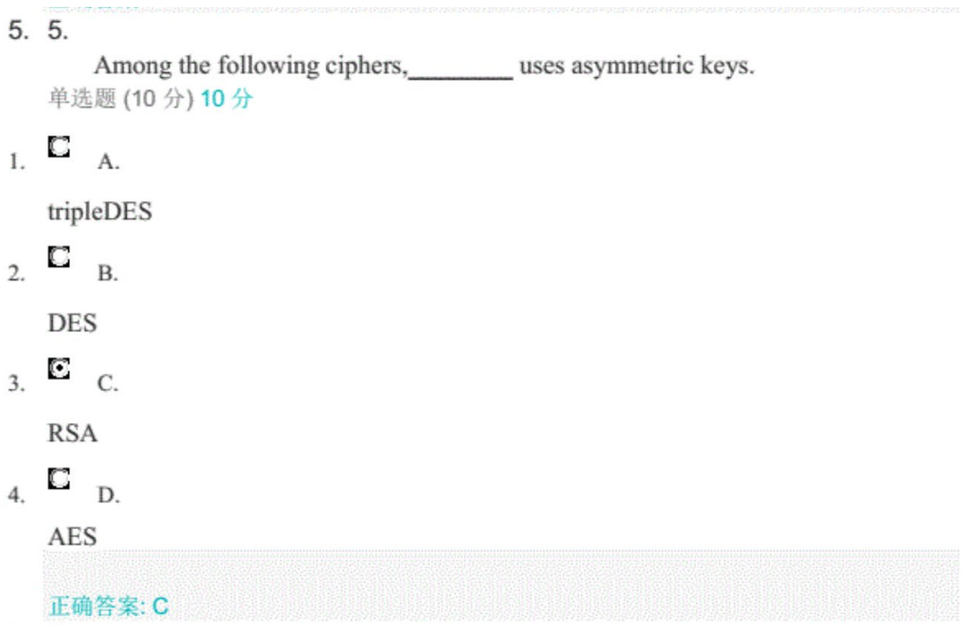
flow control

3. ○ C.

symmetric encryption algorithms

4. ○ D.

asymmetric encryption algorithms



5. 5.

Among the following ciphers,________ uses asymmetric keys.

单选题 (10 分) 10 分

1. ○ A.

tripleDES

2. ○ B.

DES

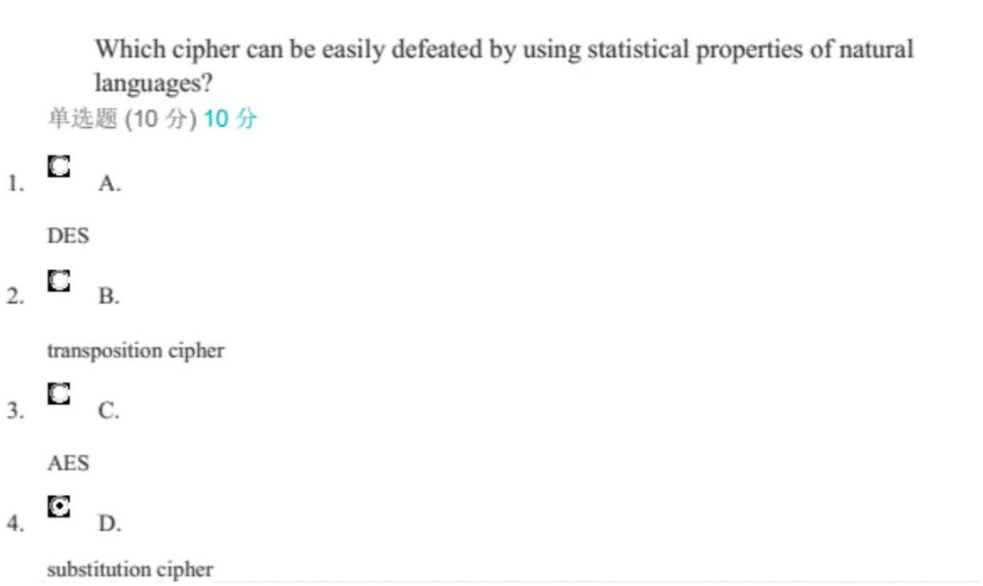
3. ● C.

RSA

4. ○ D.

AES

正确答案: C



Which cipher can be easily defeated by using statistical properties of natural languages?

单选题 (10 分) 10 分

1. ○ A.

DES

2. ○ B.

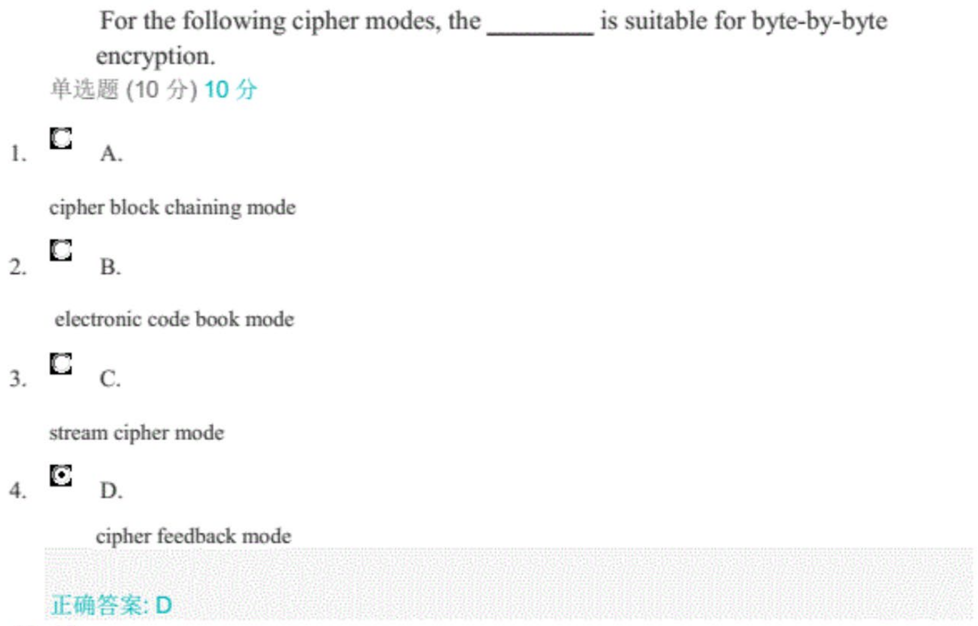
transposition cipher

3. ○ C.

AES

4. ● D.

substitution cipher



For the following cipher modes, the ________ is suitable for byte-by-byte encryption.

单选题 (10 分) 10 分

1. ○ A.

cipher block chaining mode

2. ○ B.

electronic code book mode

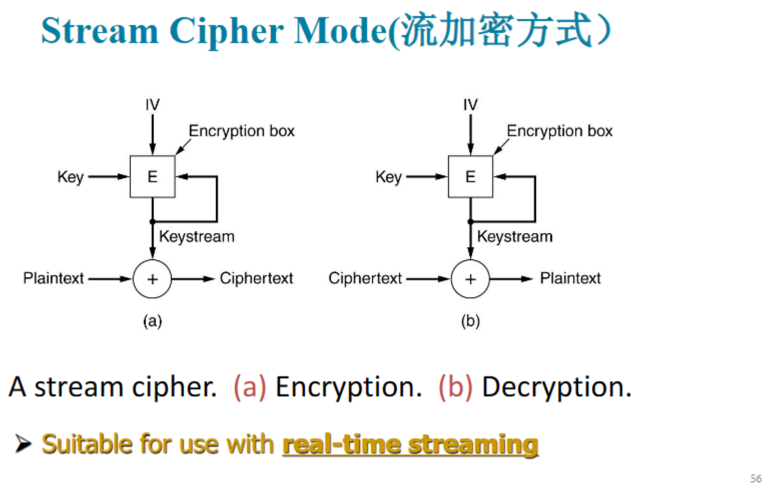
3. ○ C.

stream cipher mode

4. ● D.

cipher feedback mode

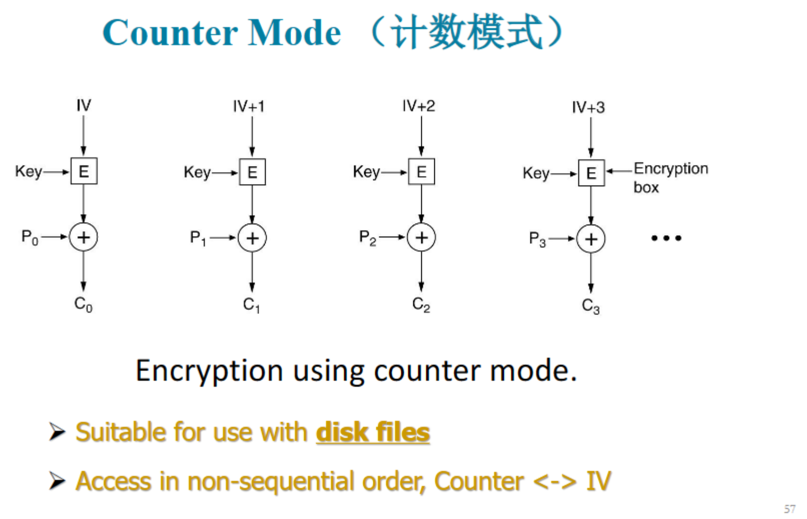
正确答案: D



Stream Cipher Mode(流加密方式)

A stream cipher. (a) Encryption. (b) Decryption.

- Suitable for use with **real-time streaming**



Counter Mode （计数模式）

Encryption using counter mode.

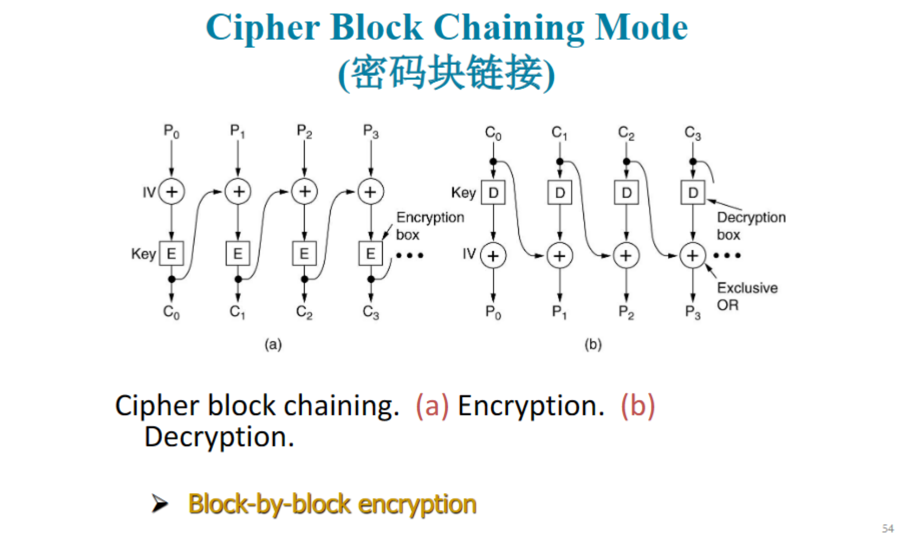
- Suitable for use with **disk files**
- Access in non-sequential order, Counter <-> IV

100. Which key will be used if A wants to send encrypted data to B when using public-key algorithms?

A. The public key of A　　B. The private key of A

C. The public key of B　　D. The private key of B

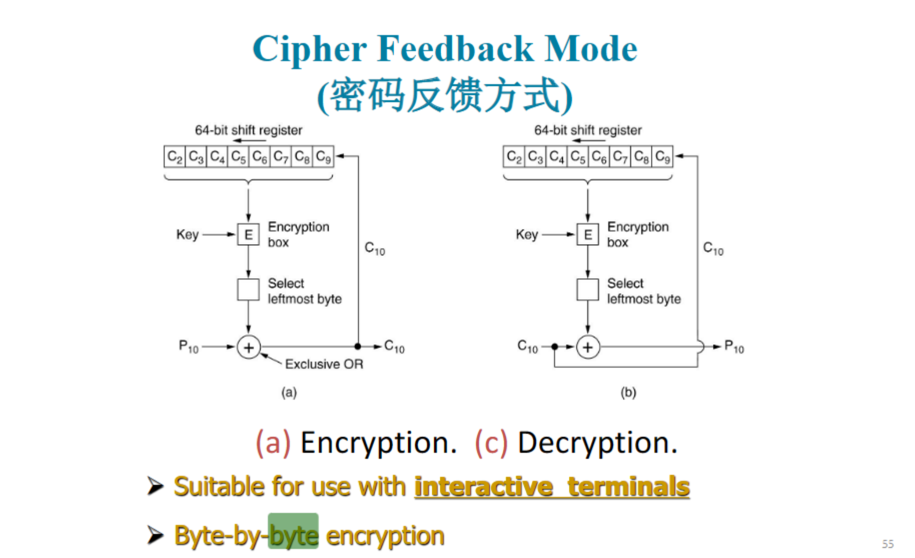
When using a public-key encryption algorithm, the sender (A) will use the recipient's (B) public key to encrypt the data. The recipient (B) will then use their own private key to decrypt the data.



Cipher Block Chaining Mode (密码块链接)

Cipher block chaining. (a) Encryption. (b) Decryption.

- Block-by-block encryption



Cipher Feedback Mode (密码反馈方式)

(a) Encryption. (c) Decryption.

- Suitable for use with **interactive terminals**
- Byte-by-byte encryption