Search for questions

Filters

Which is an invertible box?

Compression P-box

Expansion P-box

Straight P-box

S-box

What is a components of modern stream cipher?

Feedback function

Compression P-Box

Straight P-box

S-boxes

What is the **diffusion** property of Product ciphers

hide the relationship between the ciphertext & the key

hide the relationship between the ciphertext & the plaintext

hide the relationship between the key & the plaintext

hide the relationship between the round keys

Which is the objective of **hash** function?

Confidentiality

Authentication

Availability

Integrity

DES - Data Encryption Standard algorithm has block size............., key size...........

Block 64bits, key 56bits

Block 56bits, key 64bits

Block 64bits, key 58bits

Block 64bits, key 64bits

What is the size of the block and hashed message in SHA-512?

64 bits, 8 bits

1024 bits, 512 bits

64 bits, 512 bits

80 bits, 512 bits

To ensure message integrity, what solutions are used?

RSA

DES and TripleDES

Hash and MAC

AES and DES

Diffie-Hellman is used for.....

encrypt a key

exchange a secret key

decrypt a key

generate a key

Which **isnot** the operation in a round of AES?

Mixcolumns

ShiftRows

Straight P-box

SubByte

Avalanche Effect property proves DES has been to be strong, means:..........

a small change in plaintext/key => a significant change in ciphertext

a small change in the ciphertext => a significant change in the plaintext

a small change in plaintext => a significant change in the ciphertext & key

a small change in the ciphertext or key =>a significant change in plaintext

What is the size of each round key (after generated) input to every round in DES?

56 bits

32 bits

64 bits

48 bits

Diffie-Hellman is currently used in many protocols, such as: ....

TLS

TCP

IP

HTTPS

Given 2 primes: p=13, q=19, which of the values is a valid of "e" in RSA?

27

47

21

39

In asymmetric- key encryption. Bob wants to generate a signature for text M to send to Alice. Which key is used?

Alice's Private key

Alice's Public key

Bob's Public key

Bob's Private key

Assume RSA has the pubic key (7,187) and private key (23,187). Which message M= 12 will be encrypt to?

17

121

177

133

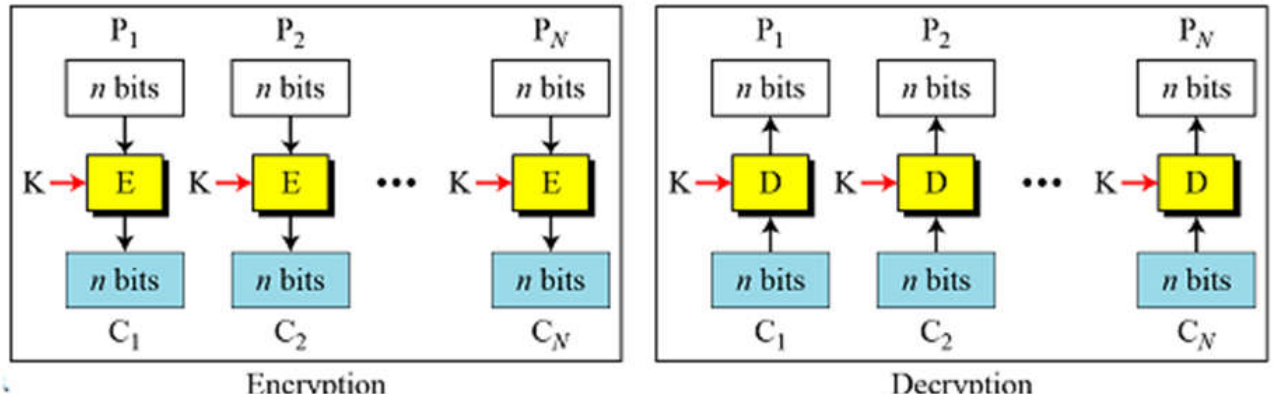
In asymmetric key cryptography. Alice needs to decrypt the text Bob sent, what key does Alice need to use?

Alice's Private key

Alice's Public key

Bob's Public key

Bob's Private key



Given below figure, which mode?

cipher block chaining mode - CBC

electronic codebook mode - ECB

cipher feedback mode - CFB

output feedback mode – OFB

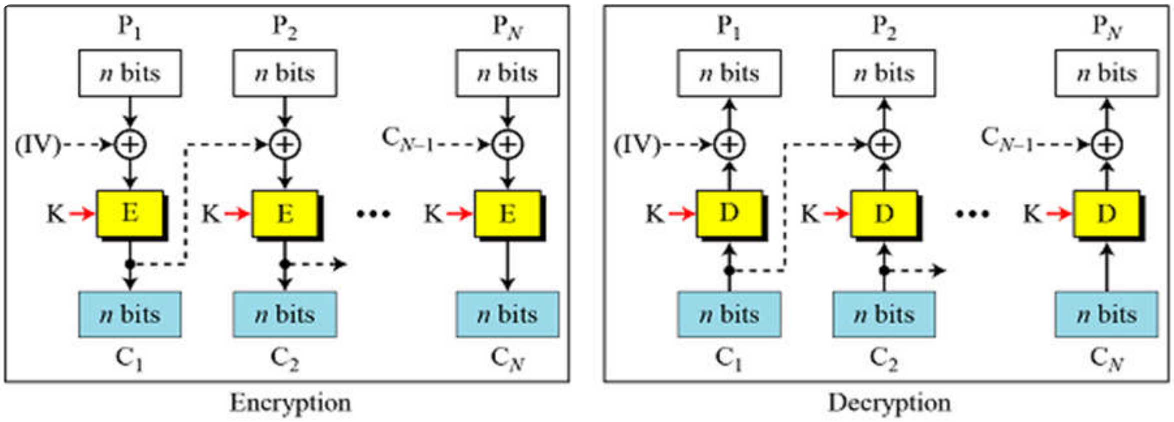
In asymmetric key cryptography. Alice encrypts message to send to Bob, what key does Alice need to use?

Alice's Private key

Alice's Public key

Bob's Public key

Bob's Private key



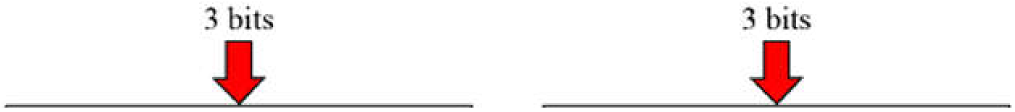
Given below figure, which mode?

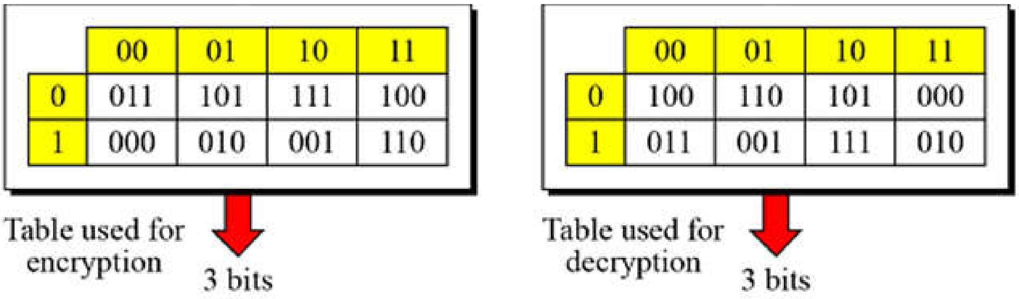
cipher block chaining mode - CBC

electronic codebook mode - ECB

cipher feedback mode - CFB

output feedback mode – OFB





	00	01	10	11
0	011	101	111	100
1	000	010	001	110

	00	01	10	11
0	100	110	101	000
1	011	001	111	010

Table used for encryption
3 bits
Table used for decryption
3 bits

Given below table for encryption and decryption. Which is the cypher of plaintext = 110?

011

100

101

001

The best way to complete your school assignments.

CHEATS

Quizizz Edpuzzle Edulastic

Kahoot Gimkit Nearpod

Blooket Wordwall

Quizlet Liveworksheets

RESOURCES

Premium

Docs

Status

LEGAL

Privacy Policy

Terms Of Service