Quick Note On Cryptography From CISSP Exam Perspective

Asymmetric uses different keys for encryption and decryption whereas **Symmetric** uses the same key for Encryption and Decryption.

Encryption Algorithm also known as cipher.
Symmetric Algorithm is either block or stream.
Asymmetric Algorithm is either discrete or factorization.

Symmetric Cryptography Key also known as private, session, secret and shared.

Key – is about how to use algorithm.
Keys are also known as crypto variable.
Plaintext + Initialization Vector + Algorithm + Key = Cipher text

IV/Salt/Nounce – Adds randomness in cipher text/Password

Work Factor – Time/efforts required to break a cryptosystem

Mono-Alphabetic Cipher - Ceasar Cipher
Poly-Alphabetic Cipher - Vignere Cipher
Both are Substitution Cipher

One Time Pad – Unbreakable Cipher if implemented properly.
Digital Signature – Hash value encrypted with sender's private key
Digital Certificate – Senders' public key signed with Digital Signature.

Computers can only generate pseudo random numbers and not pure random numbers.

Security depends on the secrecy of the key, not the secrecy of the algorithm.

Kirchokhoff's Law: Make the Algorithm Public and Key secret. where as in Security through Obscurity believes in keeping keys as well as Algorithm secret.

Symmetric Encryption: Cipher are either confusion based or diffusion based
Confusion – makes relationship between cipher text and key as complex as possible
Diffusion – dissipates statistical structure of plaintext over bulk of cipher text
Substitution – replaces one character with another. This provides confusion.
Permutation/Transposition – Provide confusion by rearranging the characters leading to diffusion.

DES Modes:

ECB: Least secure as it uses Secret Key (Static)
Suitable for exchange of small data.
No IV.

CBC: It is a block cipher
Uses IV and it has chaining.
As it has chaining; it propogates errors during encryption process.

CFB: It is a Stream Cipher
Uses IV and chaining
As it has chaining; it propogates errors during encryption process.

Quick Note On Cryptography From CISSP Exam Perspective

OFB: Stream cipher
No chaining hence it does not propogate errors.

CTR Mode: Stream cipher
It uses counter and helps in parallel computing.
No chaining.

Out of DES modes:
OFB and CTR has no chaining hence it does not propogate errors.

Block Cipher: Encrypts block by Block.

Stream Cipher: Encrypts bit by bit.
Usually incorporated with hardware.
XOR, Transposition, Substitution.
RC-4, used by WEP and WPA;
DES modes which ends FB (facebook) CFB & OFB and CTR mode; All others are block ciphers.

Cons of Symmetric Cryptographic:
Out of band key distribution
Not repudiation
Not scalable
No authenticity
Integrity
Pros of Symmetric Cryptography
FAST.

Keys Should be properly destroyed on EOF (End of Life).

Link Encryption:
Entire packet is encrypted
Hence the packets gets decrypted at every node.
If one of the node is compromised; then it may lead to breach in confidentiality.
Works at lower layers. Data link layer.
Helps when connecting two offices.

End to End Encryption:
Only payload is encrypted and not the header.
So the packet need not be decrypted on every node as header is not encrypted.
Works at Application layer.
SSH is an example of End to end encryption.