**Chapter 6: Cryptography and Symmetric Key Algorithms**

Security practitioners use cryptographic systems to meet four fundamental goals: confidentiality, integrity, authentication, and nonrepudiation.

**Work Function/ factor** represents the time and/or cost effort required to perform a complete brute-force attack against an encryption system.

**Transposition cipher** - A secret word is chosen first and written in a row. Now, columns are labeled as per the alphabetical order of characters in the secret word. The message to be encrypted is then written in a matrix with the number of columns equal to the secret word length. The matrix is then read column wise based on the column numbering done in the second step.

**Substitution cipher** - Substitution ciphers use the encryption algorithm to replace each character or bit of the plaintext message with a different character.

* **Caesar cipher** - It is a mono-alphabetic substitution cipher. It has a key length of 1. It shifts characters by 3 (ROT3).
* **Vigenere cipher** - It is a poly-albhabetic substitution cipher. The key length is usually a word or phrase (n). First n characters in the message are ROTted differently based on the alphabetical number of the characters in key. For eg - if the key is BAN then the first character of the message will be ROT(2-1), second will be ROT(1-1), and so on. The sequence is then repeated for next n (key length) characters and so on.
* **One time pad** - It uses a key of length equal to the message length. All characters in the message are shifted with different numbers. It is the only cipher which is unbreakable when implemented properly. However, the implementation is very difficult due to requiring exchange of lengthy keys.
* **Running key cipher** - Key exchange is a big problem in one time pad. In running key cipher or book cipher, sender and recipient might agree in advance to use the text of a chapter from a book beginning with the third paragraph (let's say), as the key. They can then use as many characters as required for encryption or decryption operation.

**Block ciphers** - Block ciphers operate on “chunks,” or blocks, of a message and apply the encryption algorithm to an entire message block at the same time. For eg- transposition cipher.

**Stream cipher** - Stream ciphers operate on one character or bit of a message (or data stream) at a time. For eg - Caesar cipher, one time pad, etc.

Cryptographic algorithms rely on two basic operations to obscure plaintext messages—confusion and diffusion.

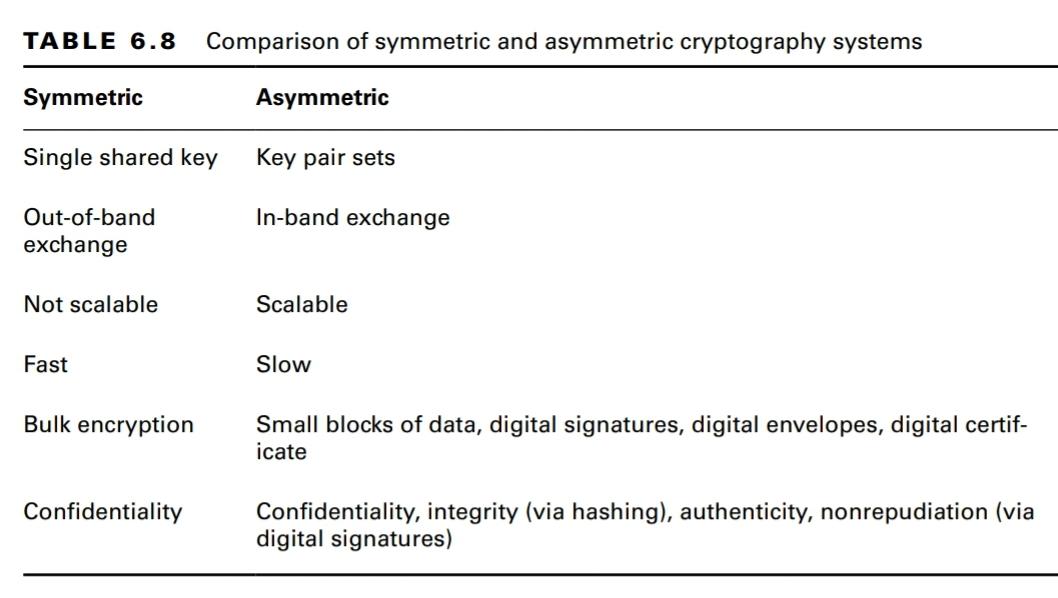
**Confusion** occurs when the relationship between the plaintext and the key is so complicated that an attacker can’t merely continue altering the plaintext and analyzing the resulting ciphertext to determine the key.

**Diffusion** occurs when a change in the plaintext results in multiple changes spread throughout the ciphertext.

Number of keys required for

* Symmetric cryptography = n(n-1)/2
* Asymmetric cryptography= 2n

For 100 people, it will require 200 asymmetric keys and 4950 symmetric keys. Due to the high number of keys required, symmetric cryptography is not scalable.



**Symmetric Cryptography - Modes of Operation**

* **Electronic Code Book (ECB)** - Simplest mode, 64 bit blocks are encrypted independently.
* **Cipher Block Chaining (CBC)** - Each block of unencrypted text is XORed with the block of ciphertext immediately preceding it before it is encrypted. For the first block, IV is used. Major consideration is that errors propagate - if one block is corrupted during transmission, it becomes impossible to decrypt that block and the next blocks as well.
* **Cipher Feedback Mode (CFB)** - It is the streaming cipher version of CBC. In other words, CFB operates against data produced in real time. However, instead of breaking a message into blocks, it uses memory buffers of the same block size. As the buffer becomes full, it is encrypted and then sent to the recipients in real time.
* **Output Feedback Mode (OFB)** - Similar to CFB, but instead of chaining it uses seed values for Xor operations. Seed value for a block is calculated based on previous seed value. For the first block, IV is used to calculate the seed value.
* **Counter (CTR) Mode** - Same as OFB, instead of seed value it uses a counter which increments for each operation.
* Galois/Counter Mode (**GCM**) - Uses the standard CTR mode of encryption + adds data authenticity controls to provide integrity.
* **CCM** mode - Combines CTR mode with CBC for data authenticity.

GCM and CCM modes both include data authenticity in addition to confidentiality. They are, therefore, known as authenticated modes of encryption.

IDEA was the patented algorithm but now it is available to use as the patent has expired.

The number of encryption rounds in AES depends on the key length chosen:

■ 128-bit keys require 10 rounds of encryption.

■ 192-bit keys require 12 rounds of encryption.

■ 256-bit keys require 14 rounds of encryption.

Rijndael uses a block size equal to the key length.

