1 Key exchange

- TLS_RSA
- TLS_DH_anon (anonymous)
- TLS_PSK (pre shared key)
- TLS_SRP (secure remote password)

Only these methods provide **forward secrecy** since the public key changes for every instance of the protocol. The last 'e' stands for *ephemeral*.

- TLS_DHE
- TLS_ECDHE

The following methods provide no authentication of server and user, hence suffers from MITM attacks, rarely used

- TLS_DH
- TLS_ECDH

Remark 1. *These methods can be combined together for instance we can have DHE_RSA, ECDHE_PSK, PSK_RSA etc.*

1.1 Secure Remote Password

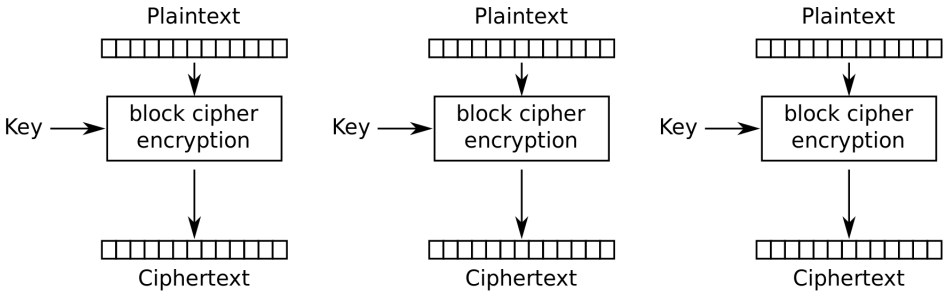
TLS_SRP provides **mutual authentication** while TLS with server certificates only authenticates the server to the client.
Moreover the user does not need to check the URL being certified since if the server does not know the password the connection can not be established. This prevent phising.
Note that using password based authentication does not require reliance of certification authorities.

2 Block cipher modes

A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block. A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block.

Most modes require a unique binary sequence, often called an initialization vector (IV), for each encryption operation. The IV has to be non-repeating and, for some modes, random as well. The initialization vector is used to ensure distinct ciphertexts are produced even when the same plaintext is encrypted multiple times independently with the same key.

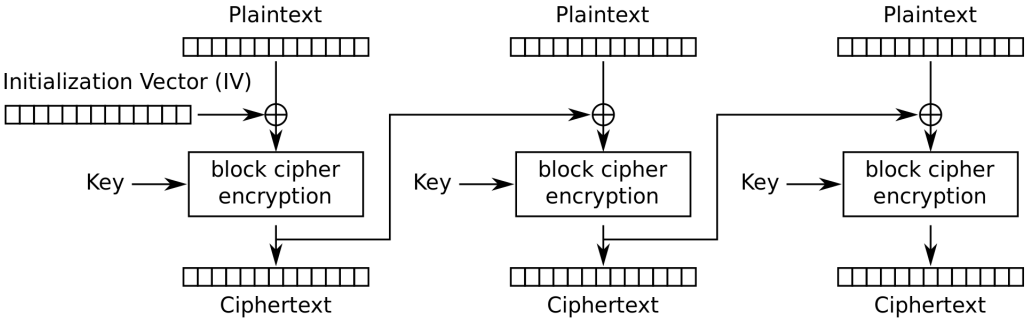
2.1 Electronic Codebook (ECB)



Electronic Codebook (ECB) mode encryption

The message is divided into blocks, and each block is encrypted separately. The disadvantage of this method is that identical plaintext blocks are encrypted into identical ciphertext blocks; thus, it does not hide data patterns well. In some senses, it doesn't provide serious message confidentiality, and it is not recommended for use in cryptographic protocols at all

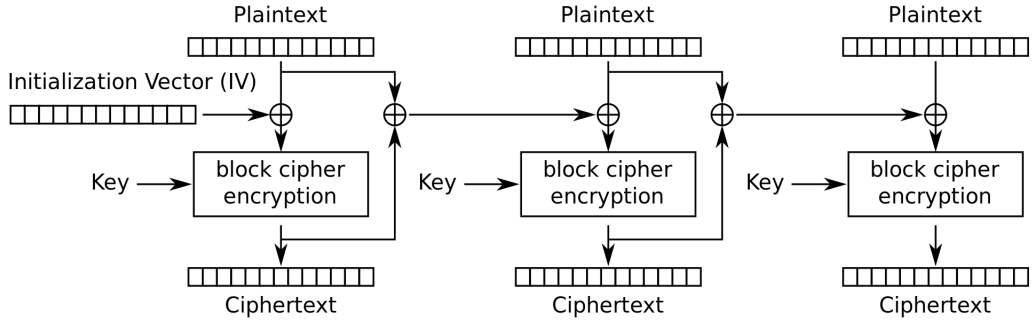
2.2 Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.

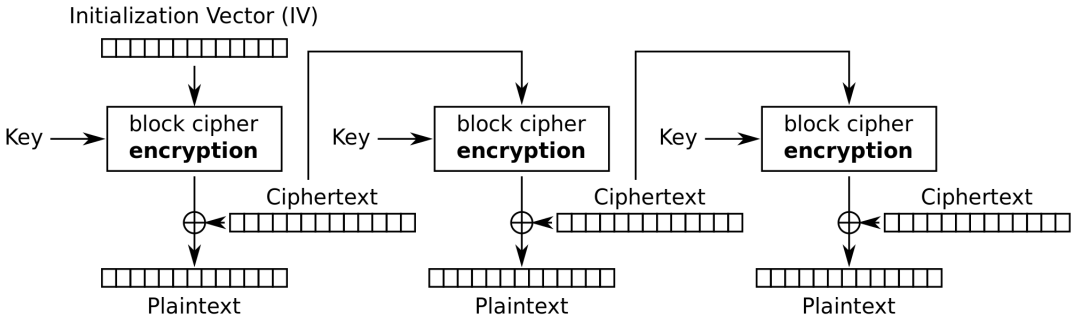
2.3 Propagating Cipher Block Chaining (PCBC)



Propagating Cipher Block Chaining (PCBC) mode encryption

In PCBC mode, each block of plaintext is XORed with both the previous plaintext block and the previous ciphertext block before being encrypted. As with CBC mode, an initialization vector is used in the first block.

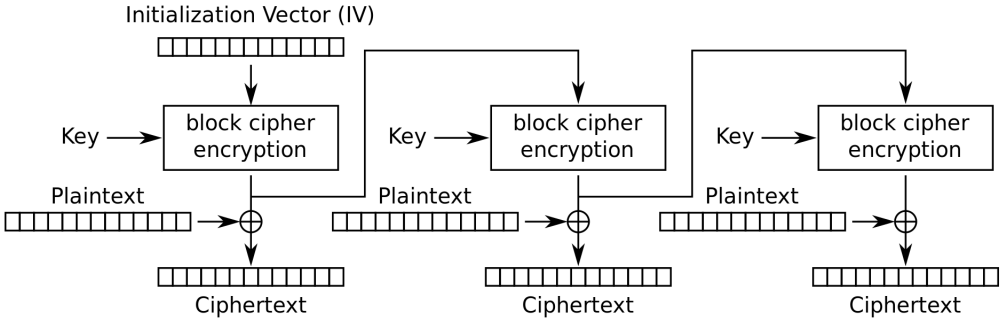
2.4 Cipher Feedback (CFB)



Cipher Feedback (CFB) mode decryption

The Cipher Feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher. Operation is very similar; in particular, CFB decryption is almost identical to CBC encryption performed in reverse. By definition of self-synchronising cipher, if part of the ciphertext is lost (e.g. due to transmission errors), then receiver will lose only some part of the original message (garbled content), and should be able to continue correct decryption after processing some amount of input data.

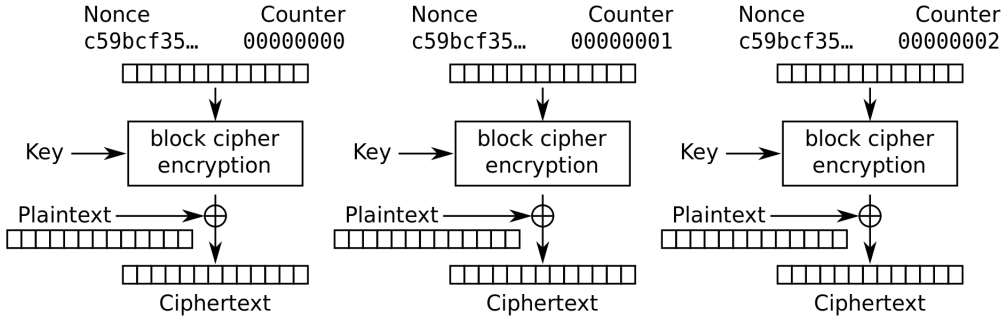
2.5 Output Feedback (OFB)



Output Feedback (OFB) mode encryption

The Output Feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption.

2.6 Counter (CTR)



Counter (CTR) mode encryption

Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.