CRYPTOGRAPHY

"crypt" = "secret" "graphy" = "writing"

Securing Information & Communication

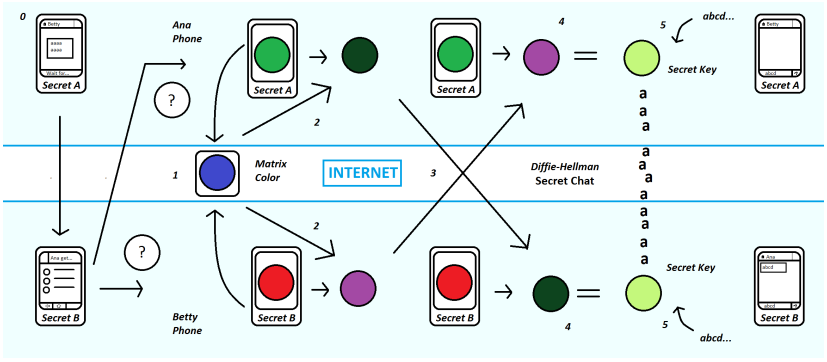
Mathematical concepts used to transform messages

Different types of algorithms are used to encrypt messages, to ensure that the messages cannot be read by the unintended user. The four objectives of cryptography are;

Confidentiality - information cannot be interpreted by anyone for whom it was unintended.
Integrity - the information cannot be manipulated.
Irrevocability - the information created and sent cannot be denied authorship.
Authentication - the receiver of the message/content can verify the identity of the sender

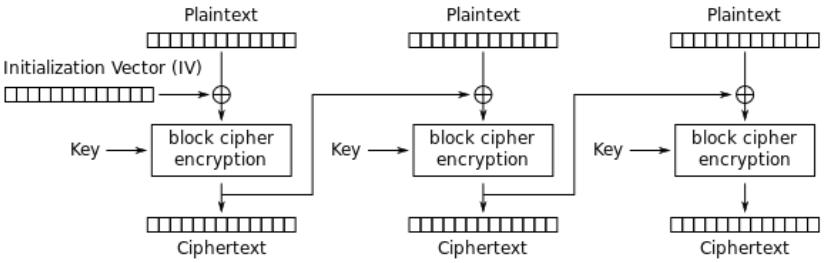
Diffie-Hellman Key Exchange - Asymmetric-key Cryptography

A method of securely exchanging cryptographic keys over a public channel. An example of this method: Alice and Bob want to communicate with each other. Alice and Bob use their private keys on an agreed upon base value that is public. They then share their computed value with each other and combine their private keys to it. The result is the secret key.

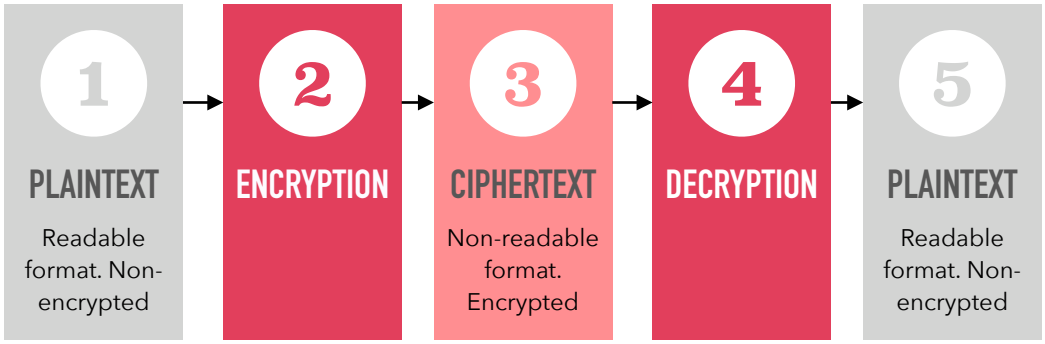


Block Ciphers & Stream Ciphers - Symmetric Key Cryptography

AES is a method of block ciphering. Encrypting blocks of data with a key and producing another block which is decrypted with the same key. Stream ciphers work by expanding a key into a pseudorandom key stream. The plaintext is then paired with the key stream using XOR to create cipher texts.



Cipher Block Chaining (CBC) mode encryption



Staying Safe

Don't reuse passwords

Keep your operating system up to date

Ensure that you are on a secure connection