



-Steganography: hiding a secret message in a secret message

-Crypto primitives:

-Cryptographic:

- 7 years after using this method some guy crack and see a hole in the method

Cryptology really encompasses two fields of research:

Cryptography - the development of cryptographic techniques

Cryptanalysis - the breaking of cryptographic techniques.

4 types of cryptoprimitives

-Block ciphers(public key) now they are block ciphers 128 bits block ciphers is common today

-Stream ciphers: encrypt bits, randomness in crypto is important,

-public-key:

-hashes

Plaintext The original format of the message

Ciphertext The encrypted form of the message

Key A parameter, input to the encryption or decryption

processes (or both)

Claude Shannon is important person