INTRODUCTION TO CRYPTO

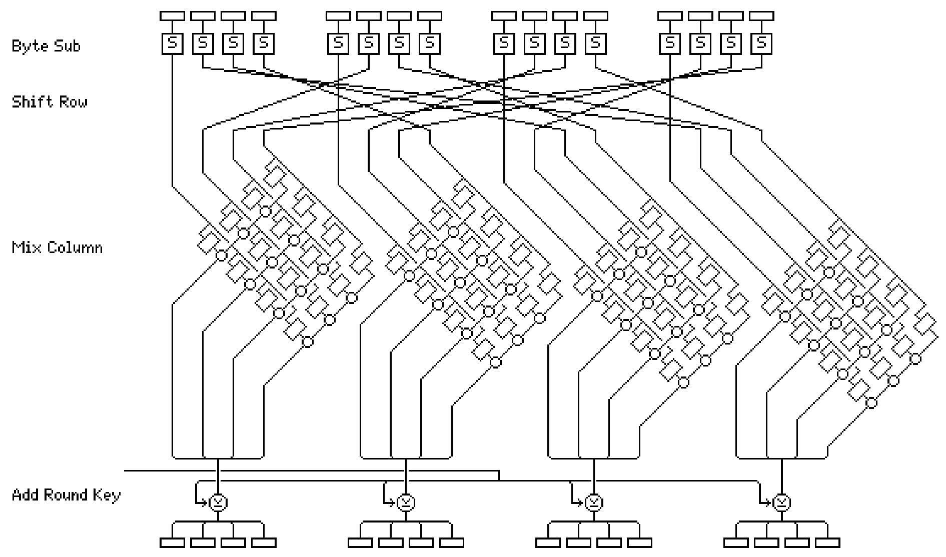
Cryptography, from the Greek kryptós+graphein meaning hidden or secret writing, is the practice and study of techniques for secure communication in the presence of third parties, called adversaries.

SECRET-KEY CRYPTOGRAPHY

Also known as "symmetric-key cryptography"

Symmetric key ciphers use the same key for encryption and decryption and work efficiently on large amounts of data. Famous symmetric key ciphers include AES, DES, and RC4.

BLOCK CIPHERS

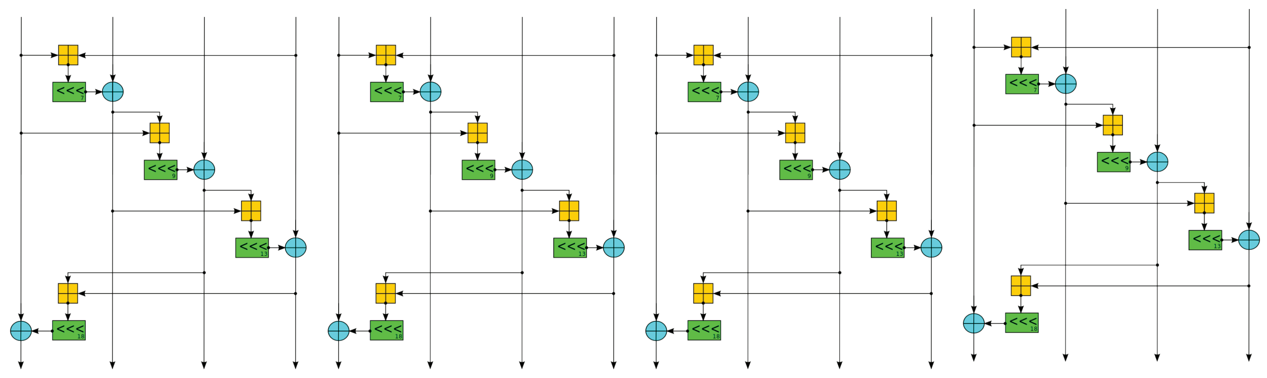


The AES Round Function

Block ciphers, as the name implies, work on fixed-sized blocks of data, encrypting a block under a given key and producing another block which can be decrypted with the same key.

Popular block ciphers include the Advanced Encryption Standard (AES) and its outdated predacessor, the Data Encryption Standard (DES)

STREAM CIPHERS



The Salsa20 Round Function

Stream ciphers work like random number generators, expanding a key into a pseudorandom keystream, then combining that keystream with the original plaintext using the XOR function to produce ciphertexts.

The most famous stream cipher is RC4, which is now known to be broken. However, newer stream ciphers like ChaCha20 are gaining popularity.

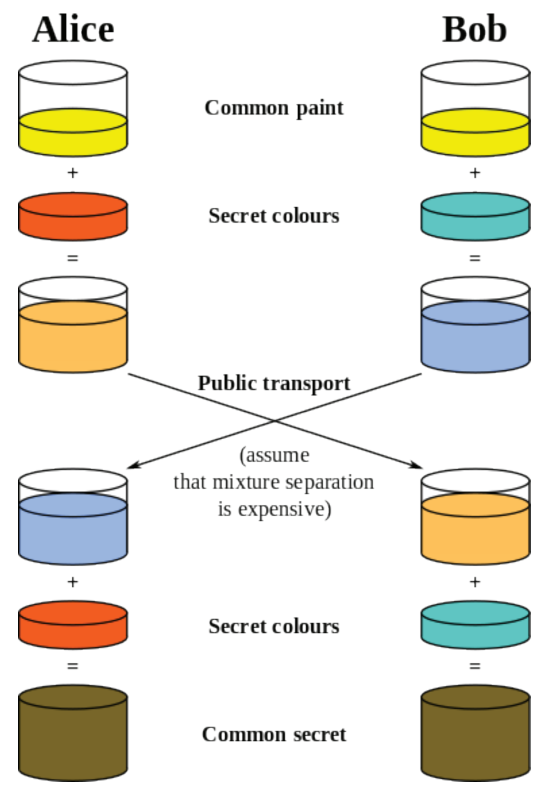
PUBLIC-KEY CRYPTOGRAPHY

Also known as "asymmetric-key cryptography"

Asymmetric key ciphers use one key for encryption (the "public key") and a different key for decryption (the "private key"). Famous asymmetric key ciphers include RSA and Diffie-Hellman.

DIFFIE-HELLMAN

Diffie-Hellman is the original public key algorithm and remains popular today in a newer, elliptic curve-based form.



Two parties mix their private keys with a base value and sharing the mixture, the public key, which can be combined to make a shared secret.

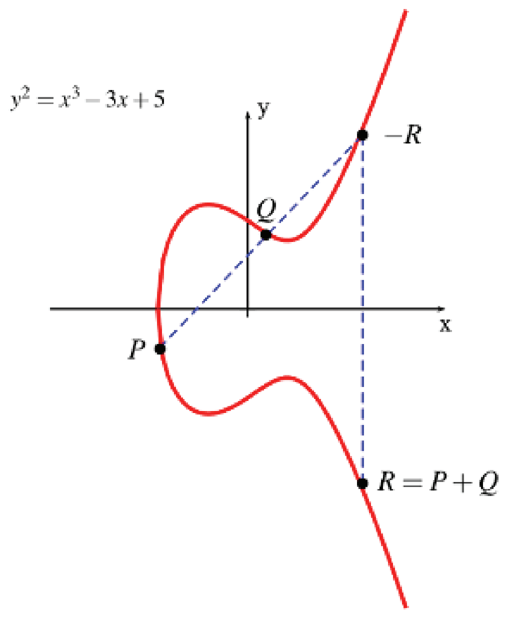
RSA

RSA is one of the most popular public key ciphers. It uses a "trapdoor function", a function that is easy to reverse if a secret value is known, but hard to reverse without it.

RSA's security relies on the intractability of factoring large numbers, as the secret value needed to solve the trapdoor function is a factor the public key. Large (2048-bit+) keys must be used to prevent the public key from being factored.

ELLIPTIC CURVE

Elliptic curves over finite fields form structures called "ladders" that allow you to easily multiply, but the reverse operation, the discrete logarithm, is costly to compute. They can be used for a faster Diffie-Hellman function.


$y^2 = x^3 - 3x + 5$
y
$-R$
Q
x
P
$R = P + Q$