Introduction to cryptography

Cryptography is the process of encrypting/decrypting data streams using some E(M)/D(M) methods.
E == encryption function
D == decryption function
M == message
C == cipher text encrypted

The root password for 204.22.3.4 is j@a83jae

Encryption function
AHHJHJJSJ
HHUSDHASA
HE8U3278
DEFDSASA

Little history about crypto

Substitution cipher
A substitution cipher is one in which the units of the plaintext (usually letters or numbers) are replaced with other symbols or groups of symbols. The actual order of the units of the plaintext is not changed.
The most known is Caesar cipher and ROT13.
Example:
GREEN FLIES ⇒ HSFFO GLJFT
Caesar Cipher

More .... (transposition)

Transposition ciphers rearrange the letters of the plaintext without changing the letters themselves. For example, a very simple transposition cipher is the rail fence, in which the plaintext is staggered between two rows and then read off to give the ciphertext. In a two row rail fence the message MERCHANT TAYLORS' SCHOOL becomes:

MRHNTYOSCOL
ECATALRSHO
Which is read out as: MRHNTYOSCOLEATALRSHO.

And more ... (polyalphabetic)

Polyalphabetic substitution cipher (Block cipher) (Vigenere cipher). t= 3 (which means each letter is mapped to three positions to its right in the alphabet, then to seven positions, and then ten positions)

M = THI SCI PHE RIS CER TAI NLY NOT SEC URE
C = WOS VJS SOO UPC FLB WHS QSI QVD VLM XYO
And more ... (product ciphers)

It's a combination of substitution and transposition cipher.

\[ E_c(m) = m \oplus k \]

\[ E(m) = (m_0m_1m_2m_3m_4m_5m_6m_7) \]

\[ 0 \oplus 0 = 0; 0 \oplus 1 = 1; 1 \oplus 0 = 1; 1 \oplus 1 = 0 \]

Example:

- \( K = 255_{10} = 0xFF = 11111111_2 \)
- \( M = "BOOOOB" \text{(ASCII)} \)
- \( 'B' = 66_{10} = 01000100_2 \text{ xor } 11111111_2 = 01101000_2 = 68 \) = 'd'
- \( 'O' = 79_{10} = 01001111_2 \text{ xor } 11111111_2 = 00110000_2 = 60 \) = 'd'
- \( C = "cc" \text{ xor } "" = "cc" \)

And last ... (stream cipher)

Basically block ciphers with each encryption transformation change for each symbol of plaintext being encrypted.

**Vernam Cipher**

\[ E_k(m) = m \oplus k, 1 \leq i \leq t \]

If the key string is randomly chosen and never used again, the cipher is called **one-time system** or **one-time pad**.

Symmetric ciphers

All of those we just discussed. (Enigma was one of them — polyalphabetic with rotors)

Problems with them:

- Key distribution (0 and Q must meet in secrecy)
- What if T wants to communicate too? Q must create another key. Comes out that for five members we have 10 keys. [Keys = \( n(n-1)/2 \)].
- Solution: Public keys!
Public keys

Public keys crypto is based on the idea that a user can have two keys – a private key and a public key. Public is used only to encrypt the plaintext while the private is only used for decrypting. We will assume that there is no way to derive the private key from the cipher-text encrypted using the public key.

\[ E_k(m) = c \]
\[ D_k(c) = m \]

Public key – problems.

\[ E' \]
\[ E \]
\[ C' \]
\[ C \]
\[ E \]

Sender (encrypts using public key)

Receiver (decrypts ciphertext using private key)

Need for authentication

- Have a third party giving out public keys (not good)
- Have a repository called public file. This public file would have the public keys for other entities.
RSA (generating key)

RSA (Rivest-Shamir-Adleman (RSA) Algorithm)

- Uses a pair of prime numbers so large that factoring is beyond all computing capabilities.
- Here is algorithm:
  - Take two primes, \( p \) and \( q \), take their product \( n = pq \). \( N \) is called modulus.
  - User chooses a number \( e \), with no common factors (except 1) and less than \((p-1)(q-1)\). Then another number is found, using the extended Euclidean algorithm:
    \[
    (ed - 1) \mod (p-1)(q-1) = 0
    \]
  - \( e \) is called public exponents, \( d \) is called private exponent.
  - The public key is the pair \( n \) and \( e \).
  - The private key is the pair \( n \) and \( d \).

RSA (encrypting)

1. The receiver \( M \) distributes his/her public key
2. The sender \( F \) composes the ciphertext \( (c) \) from \( m \):
   \[
   c = m^e \mod n \quad (e \text{ and } n \text{ are } M \text{ public keys})
   \]
3. \( F \) sends the ciphertext \( (c) \)
4. The receiver \( M \) decrypts the message:
   \[
   m = c^d \mod n
   \]

RSA (example)

\( p = 5, \ q = 11; \ n = 55 \)

The least common multiple of \((p-1)(q-1)\) is 20.

Let \( e = 7 \).

\[
(ed - 1) \mod (p-1)(q-1) = 0, \ d = 3
\]

Let \( m \) (message) = 2

\[
c = m^e \mod n = 2^7 \mod 55 = 18
\]

To decrypt:

\[
m = c^d \mod n = 18^3 \mod 55 = 2
\]
Summary


There is a lot more, but needless to say, it would require a whole semester.