Cryptography

To insure the privacy of transmitted messages, the data can be encrypted.

Cryptography:
The study of methods to encrypt data.

Cryptanalysis:
The study of methods to decode encrypted data.

Conventional (or Single Key) Encryption:
A simple algorithm is used to transform the data.

Substitution Cipher:
Each data element is substituted with a different data element (or symbol).

Example: Caesar's Method:
Replace every letter in the alphabet with the letter 3 away from it:

A –> D
B –> E
C –> F
...
X –> A
Y –> B
Z –> C

Other substitution ciphers assign random substitutions, so that they are a bit harder to crack.

How does the receiver decode the message?
Answer: The sender needs to send the key to the receiver.

Public-Key Encryption

- Uses 2 keys - a **public key** and a **private key**.

- The receiver publishes its public key which is used by the sender to encrypt the message.

- The receiver uses the second (and different) private key to decrypt the message.

What is the relationship between the two keys?

It should be computationally infeasible to obtain the private key from a knowledge of the public key and the transmitted message.

These methods are based on the fact that it is computationally easy to multiply two large numbers, but it is quite difficult to factor a large number if it has very few factors, especially, if the factors are large prime numbers. (e.g., Try to factor 3233.)

Advantage of Public-Key Systems:

Only the public key is distributed.

Sample Public-Key Systems:

RSA - Rivest, Shamir, and Adelman
DSA - Digital Signature Algorithm
PGP - Pretty Good Privacy - uses both conventional and public-key cryptography.

PGP

Encoding Method:

1. Compress the message

2. Create a **session key** that is used only during this session. The key is created randomly from mouse movements and key strokes.

3. The session key is used to conventionally encrypt the message.

4. The receiver's public key is used to encrypt the session key.

5. The encrypted message and the encrypted session key are transmitted to the receiver.

Decoding Method:

1. The receiver uses its private key to decrypt the session key.

2. The session key is used to decrypt the message.

3. The data is decompressed.

4. The session key is discarded.

Advantages:

- Only a small amount of information (the session key) is publically encrypted.

- The session key is used only once.

- Conventional encryption can be ~10,000 faster than public-key encryption.

PGP Method

PGP uses the RSA public-key method:

M = the message
C = the encrypted message

e = the public exponent (public-key)
d = the private exponent (private key)
n = a very large integer

Encryption Method:
$C = M^e \bmod n$

Decryption Method:
$M = C^d \bmod n$

where
$n = p * q$
p and q are large prime numbers
$d = e^{-1} \bmod ((p-1) * (q-1))$

- If n is a large number (128 bits or 256 bits), it is computationally infeasible to find p and q.
  - must find all factors of n.
  - must determine which are prime.
  - must try all pairs of primes to find p and q.

Digital Signature

- Used to verify that the “sender” actually sent the message.

- The receiver publishes its public key which is used by the sender to encrypt the message.

- The sender then uses its private key to encode the encrypted message. (This is a second level of encryption.)

- The receiver first uses the sender’s public key to decrypt the message.

- The receiver then uses the receiver’s private key to fully decrypt the message.