Introduction to Cryptography

Introduction to IT Security

Otago Polytechnic
Dunedin, New Zealand

Cryptography

Cryptography is the practice of techniques for secure communication in the presence of third parties. In particular it is about the use of algorithms or protocols used for secure communication.

Typical uses of cryptography

- Secure communication (including storage)
- Authentication
- Non-repudiation

The classic process

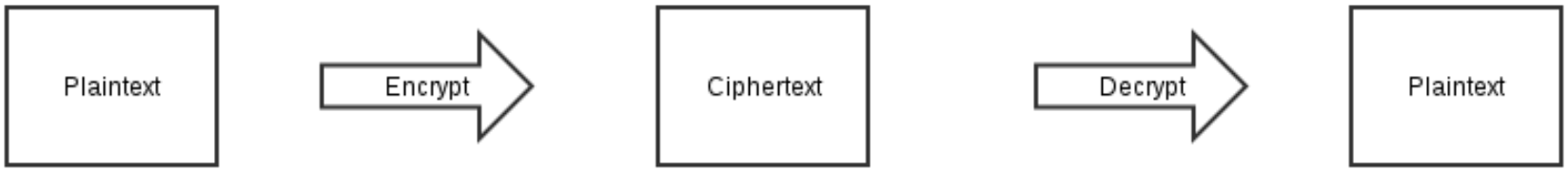

Figure: To perform the encryption/decryption processes, *keys* are required.

Some key words

Algorithm: the method by which we encrypt and decrypt a message

Key: a secret used to carry out the algorithm

In order to use encryption, we need to know the algorithm and the key.

Example: Caesar cipher

- Take the letters A through Z, ignoring lower case.
- Shift the letters n places to the right, wrapping at the end of the alphabet.
- e.g., if $n = 3$, A $\rightarrow$ D, B $\rightarrow$ E, ... Y $\rightarrow$ B, Z $\rightarrow$ C.
- In this example, the shifting is the algorithm, and the value of n is the key.

Kerckhoffs's principle

- A cryptographic system should be secure if everything about the system, except the key, is public knowledge.
- This principle is widely accepted by cryptologists. Why?
- How secure is the Caesar cipher, according to this principle?

Bitwise encryption

Classical encryption is concerned with converting between plaintext and ciphertext, but modern encryption systems generally operate on data as bits.

Example: XOR

```
plaintext:   110010110     ciphertext:  010110001
key:         100100111     key:         100100111
             ---------                  ---------
ciphertext   010110001     plaintext:   110010110
```

How secure does this seem?

Symmetric encryption

- In symmetric encryption algorithms, the same key is used for encryption and decryption.
- Symmetric algorithms are generally computationally efficient and they can be very secure.
- The main problem with symmetric algorithms is key management.

Asymmetric encryption

- In asymmetric encryption algorithms, different keys are used for encryption and decryption.
- Asymmetric algorithms are generally more computationally expensive than symmetric ones.
- Key management is simpler:
  - To send me a message securely, encrypt it with my *public key*, which I share freely. Only my *private key* can decrypt the message, but only I hold that key.
  - If I encrypt a message with my private key, then you can decrypt it with my public key - and so can anybody else. However, since only I have the private key, I **must** have sent the message.

Questions?

Today's lab: Using PGP.