Lecture 19

We now draw some lessons from our previous examples.

Kerckhoff's principle

We should never assume that the encryption algorithm used is secret.

Thus we should always work on the assumption when evaluating a crypto system that Eve knows what it is but that the keys are kept secret.

Sufficient key space principle

A secure cryptosystem must have a key space (= set of all possible keys) that is not vulnerable to exhaustive search.

Clearly, Caesar ciphers are hopeless in this regard.

If we want to determine how secure a cryptosystem is, then we need to know what information Eve can get hold of. There are two examples.

Ciphertext-only attack Eve only has examples of ciphertext. We have seen that Caesar ciphers can easily be broken using only the ciphertext.

Known plaintext attacks Here Eve has knowledge of (plaintext, ciphertext) or several such pairs. We have seen that affine block ciphers can be easily broken using known plaintext attacks.

> Affine block ciphers are too "nice" to be the basis of secure cryptosystems

I should add that other types of attack are possible — but I shall leave you to read up on this topic if you wish.

One-time pads

There is a perfect cryptosystem (but .....)

The key is a random sequence of letters of the same length as the cleartext. Encryption is addition of numerical equivalents mod 26 and conversion back to letters.

Example

Cleartext: O N E T I M E P A D

Key: T B F R G F A R F M

Ciphertext: H O J K O R E W F P

But... the key is as long as the cleartext, has to be truly random, and must never be used again.

Used, allegedly, by spies in WW2, this is not a practical cryptosystem for day to day use but is completely secure.

All the systems we have described so far belong to the class of symmetric (or classical) cryptosystems.

In such a system, the decryption key d is either equal to the encryption key e or can be quickly calculated from it.

However, there is a problem - if Alice and Bob want to communicate using a symmetric cryptosystem how do they exchange the secret key e? They certainly can't send it along the communication channel (because Eve could intercept it and then all will be lost).

This problem was only solved in the 1970's by Diffie and Hellman.