Chapter 1

Introduction

The desire for secret communications has been around for as long as human beings have been communicating. However, the earliest recorded use goes back to approximately 1900 BC when an Egyptian scribe used non-standard hieroglyphs in an inscription in order to conceal their meaning. It is true to say that the course of history has been shaped by secret communications and that the lives of Kings and Queens have on many occasions, been in the hands of these communications. The strength of the methods used to obtain secrecy was often the deciding factor in a life or death situation.

Today the need for private communications has increased dramatically. With the advent of the Internet, secure communications has become a must for people wishing to keep their privacy intact. The main tool used to ensure this privacy is known as **cryptography** - the art of secret writing.

1.1 Brief overview of cryptography

The idea of cryptography is to convert information to a form that will be unintelligible to an unintended recipient. It accomplishes this using a cryptographic algorithm known as a **cipher**, and an object known as a **cryptographic key**. The information to be converted is known as **plaintext** and the converted information is known as **ciphertext**. The process of converting plaintext to ciphertext is known as **encryption** and the process of converting back from ciphertext to plaintext is known as **decryption**. The cryptographic key may or may not be the same for both encryption and decryption depending on the type of algorithm used.

There are two main types of cryptography in use today - **symmetric** or **secret key** cryptography and **asymmetric** or **public key** cryptography. Symmetric key cryptography is the oldest type whereas asymmetric cryptography is only being used publicly since the late 1970's[1]. Asymmetric cryptography was a major milestone in the search for a perfect encryption scheme as will be seen.

The subject of breaking ciphers is known as **cryptanalysis** and a person in the business of breaking ciphers is known as a **cryptanalyst**. Cryptographers (people who try to devise secure ciphers) and cryptanalysts have been working against each other since the Arabs invented cryptanalysis around AD 800. The combined studies of cryptography

[1] It is claimed by some that government agencies knew about asymmetric cryptography before this.

and cryptanalysis is known as **cryptology**.

1.2 Security concepts

In an organisation wishing to keep its information secure it will generally tend to use cryptography. However, security in general needs to be overviewed without reference to any particular method. Three types can be looked at: Computer security, Network Security and Internetwork security. The third one is of concern here and consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information across interconnected networks. Three aspects of security need to be considered when assessing the security needs of an organisation:

1. **Security service**: A service that enhances the security of the data processing systems and information transfers.
2. **Security attack**: Any action that compromises the security of information owned by an organisation.
3. **Security mechanism**: A mechanism that is designed to detect, prevent or recover from a security attack.

One useful classification of security services is as follows:

- **Confidentiality**: Requires that information be accessible only by authorised parties.
- **Authentication**: Requires that the origin of a message be correctly identified with the assurance that the identity is not false.
- **Integrity**: Requires that system assets and transmitted information be capable of modification only by authorised parties.
- **Non-repudiation**: Requires that neither the sender nor receiver of a message be able to deny the transmission.
- **Access Control**: Requires that access to information resources be controlled by or for the target system.

Security attack consist of four general categories:

1. **Interruption**: A system asset is destroyed or becomes unavailable - an attack on the **availability** of a system.
2. **Interception**: An unauthorised party gains access to an asset. This is an attack on **confidentiality**.

3. **Modification**: An unauthorised party not only gains access to an asset but tampers with it. This is an attack on **Integrity**.
4. **Fabrication**: An unauthorised party inserts counterfeit objects into the system. This is an attack on **authenticity**.

It might also be useful to categorise the attacks in terms of active and passive attacks:

- **Passive attack**: Passive attacks involve monitoring data transmissions without modification of the data stream. The main aim is to **prevent** this form of attack as detection is difficult.
- **Active attack**: Active attacks involve some modification of the data stream or the creation of a false stream. With active attacks the main aim is to **detect and recover** as prevention is difficult.

There is no single mechanism that will provide all of the services outlined above - a variety of mechanisms come into play. However, there is one element which underlies most security schemes in use: cryptographic techniques. This course looks at the development, use and management of such techniques.

1.3 Conventional Encryption

Conventional encryption (also termed single-key or symmetric encryption) was the only form of encryption until public-key algorithms were introduced in the mid 70's. It is still the dominant form used today. Figure 1.1 illustrates the conventional encryption model and figure 1.2 allows us to take a closer look at the essential elements of conventional encryption.

Here we can see that the message source produces the **plaintext** message of the form

$$P = [p_1, p_2, \ldots, p_m]$$

the m elements are letters of some alphabet, traditionally 26 letters and now just $\{0, 1\}$. For encryption, a **key** is generated of the form:

$$K = [k_1, k_2, \ldots, k_j].$$

If generated at the source, the key must be available at the destination by means of some secure channel, or a third party securely deliver to source and/or destination.

The encryption algorithm (or **Encrypter**) using the message P and the key K forms the ciphertext

$$C = [C_1, C_2, \ldots, C_m]$$

expressed as

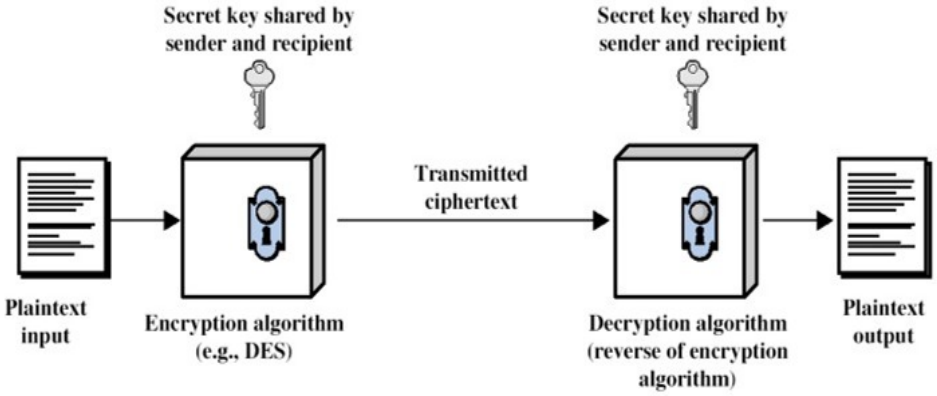

Figure 1.1: Simplified model of conventional encryption.

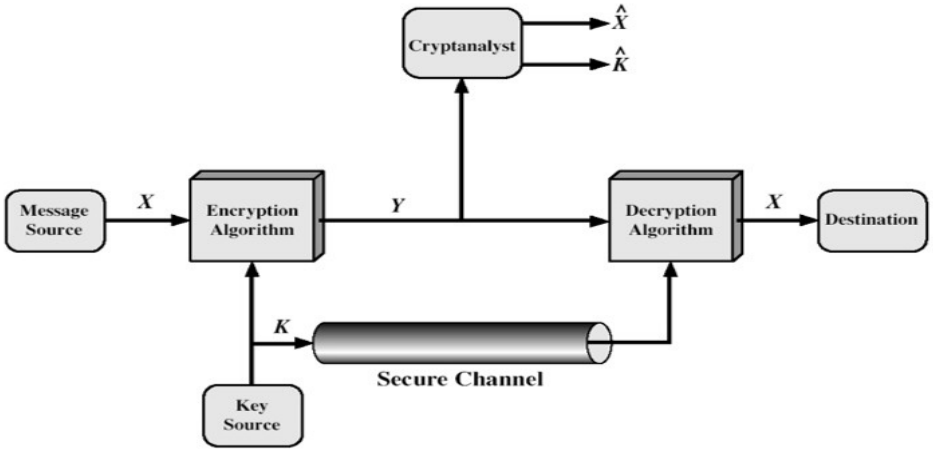

Figure 1.2: Closer look at the essential elements of a conventional cryptographic system. In this case X = P and Y = C. The values $\hat{X}$ and $\hat{K}$ are estimates of the plaintext and key.

$$C = E_k(P). \tag{1.1}$$

The intended receiver in possession of the key is able to invert the transformation

$$P = D_k(C). \tag{1.2}$$

An opponent, observing C but not having access to P or K must recover one or both

assuming he has knowledge of E and D. He may want to generate an **estimate** of the current message P or to discover future message by estimating K.

1.4 Classical Encryption Techniques

Although these techniques are of little direct interest for modern security applications, an overview enables us to illustrate some of the basic approaches to encryption used today and some of the attacks that must be anticipated.

- **Substitution technique**: This is one in which the letters of the plaintext are replaced by other letters or symbols (e.g. The Caesar Cipher).
- **Transposition technique**: This is where the letters are reorganised but are not replaced by other letters.

The **Caesar Cipher** is the earliest known (and the simplest). It involves replacing each letter of the alphabet with the letter standing three places further down. This is then wrapped around on itself when the end is reached. For example:

Plaintext:	meet	me	after	the	party	is	over
Ciphertext:	PHHW	PH	DIWHU	WKH	SDUWB	LV	RYHU

Assigning numbers to the alphabet ($a = 1, b = 2$ etc.) for plaintext letter p, substitute ciphertext letter C. We have encryption function E:

$$C_i = E(p_i) = (p_i + 3) \bmod 26$$

Although documented accounts of the Caesar cipher show Caesar only using a shift of three, it is very likely that he used other shifts as well. In the general case then, the encryption function would be:

$$C_i = E(p_i) = (p_i + k) \bmod 26 \qquad 1 \leq k \leq 25$$

The decryption function D is simply:

$$p_i = D(C_i) = (C_i - k) \bmod 26 \qquad 1 \leq k \leq 25$$

Brute-force cryptanalysis is easily performed on the Caesar cipher by trying all 5 possible keys. The plaintext becomes evident at the third iteration in this instance.

Three characteristics of the problem facilitate the successful use of the brute force approach:

1. The encryption scheme is known

2. There are only a limited no. of keys
3. The plaintext is easily recognisable

In most situations the algorithm is known and the key size tends to be the main problem for brute-force attacks. For example DES (symmetric cipher to be covered later in the course) has a 56 bit key so there are only 2^{56} options (to make matters worse, on average only half of them will need to be searched).

Monoalphabetic Ciphers: If instead of using only the 25 possible keys, arbitrary substitution is used, then there are $26!$ or $4 \times 10^{26} \approx 2^{88}$ possible keys (10 orders of magnitude greater than the keyspace for DES!). This makes a brute force very difficult without very large resources. Another line of attack is if the cryptanalyst knows the nature of the plaintext (say English text). In this case regularities of the language may be exploited. For example, the relative frequency (%) of letters in English text can be seen in figure 1.3 where it can be seen that the letters E, T and A are the three most used letters in the English language.

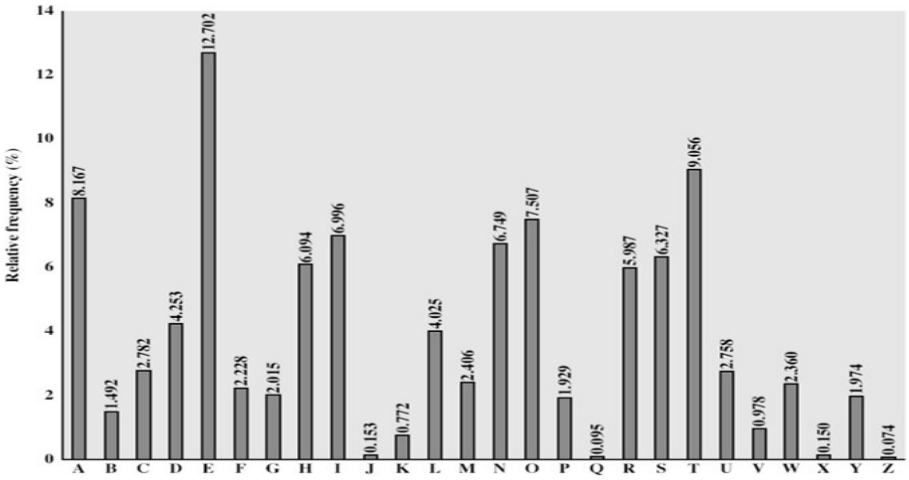

Figure 1.3: Relative Frequency of letters in the English Language.

Of course not all relative frequencies will end up as in figure 1.3. That particular graph is calculated over a very large sample space however it is possible to use it to assist in deciphering the text. Given an encrypted text, the relative frequency of the encrypted letters could be determined and then compared with figure 1.3. Intelligent guesses could then be made at what the plaintext is.

Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet. Gauss believed that he had an unbreakable cipher when he came up with the countermeasure to provide multiple substitutes for a single letter (known as homophones).

Homophones : For example we could assign 4 or 5 different symbols to the letter 'e' etc. to be used in rotation and match the number of symbols allocated to each letter to their relative frequency, then any information discernable form frequency distribution is obliterated. The flaw is that multiple letter patterns (i.e. 'the') still survive (digraph frequencies) making cryptanalysis easy.

Two methods are used in substitution ciphers to lessen the extent to which the structure of the plaintext survives in the ciphertext:

1. **Multiple letter encryption**: the best known cipher of this type is "Playfair" which treats digraphs in plaintext as single units and translates these as ciphertext digraphs. Note that there are $26 \times 26 = 676$ digraphs vs. 26 letters. This was used up to WW2 by the UK and US armies but is now considered trivial because of the frequency distribution.

2. **Polyalphabetic ciphers**: Using different monoalphabetic substitutions while moving through the plaintext. The "Vigènere" cipher is the best example.

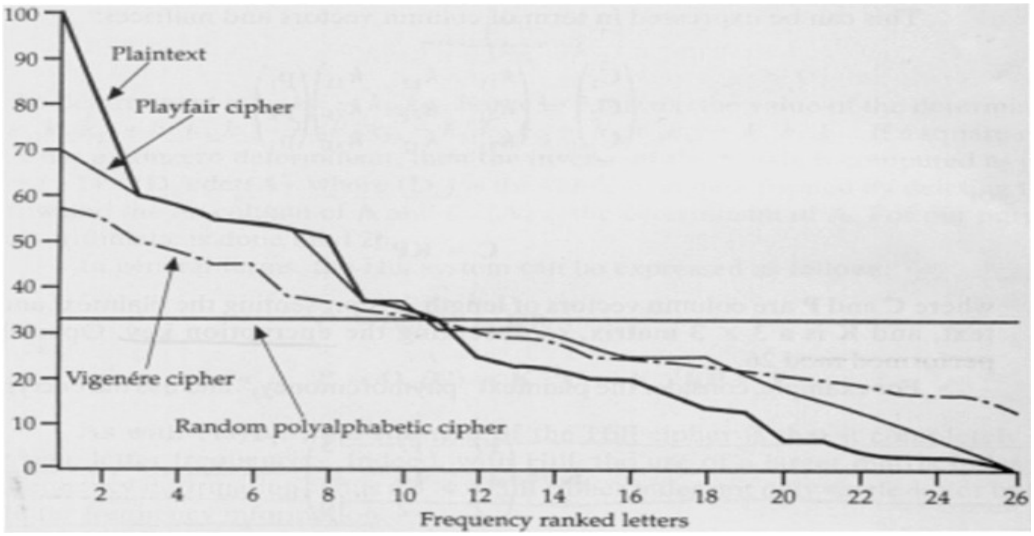

Figure 1.4: Relative Frequency of the occurrence of letters.

Transposition techniques: So far all the ciphers we have looked at involved only substitution. A very different kind of mapping is achieved using transposition. In its simplest form, the **rail fence** technique involves writing down the plaintext as a sequence of columns and the ciphertext is read off as a sequence of rows. For example, if we use a rail fence of depth 2 with the plaintext *meet me after the party is over* we get:

m	e	m	a	t	r	h	p	r	y	s	v	r
e	t	e	f	e	t	e	a	t	i	o	e	

Therefore the ciphertext is *mematrhprysvretefeteatioe* which is simply the first row concatenated with the second.

Complexity may be added by writing the message row by row and reading off column by column but permuting the order of the columns using a key. Cyrptanalysis is trivial but more than one stage helps.

Rotor Machines: The previous work suggests that multiple stages of encryption can result in an algorithm that is significantly more difficult to cryptanalyse. This is as true for substitution as it is for transposition ciphers. Before the arrival of DES the most important application of this principle was a class of systems known as Rotor machines. Rotor machines were used by both Germany (Enigma) and Japan (purple) in WW2 and the breaking of both codes was a significant factor in the war's outcome. Figure 1.5 illustrates the basic principles:

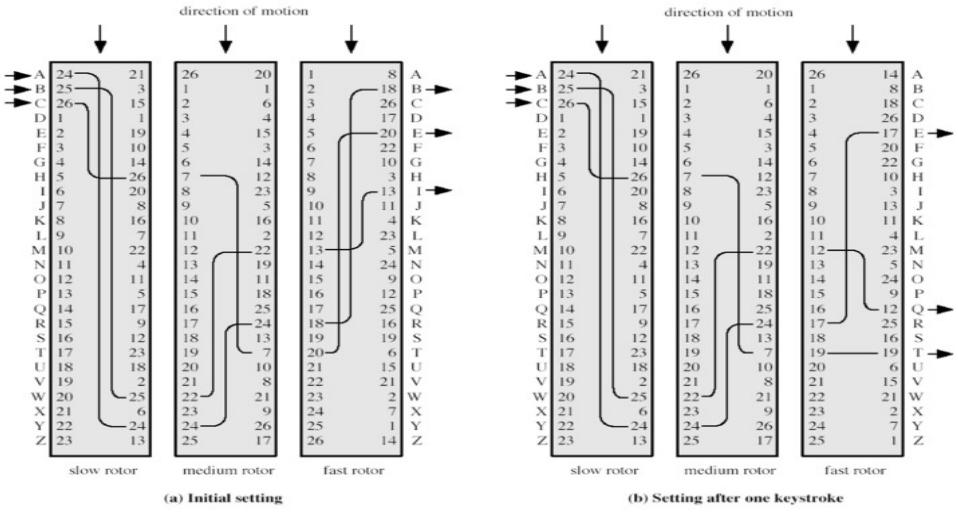

Figure 1.5: Three Rotor machine with wiring represented by numbered contacts.

- The system consists of a number of independently rotating cylinders through which electrical pulses can flow.
- Each cylinder has 26 input pins and 26 output pins with internal wiring that connects each input to a unique output, e.g. a monoalphabetic substitution (for simplicity only three connections are shown in the figure.)

- Now, consider a machine consisting of one cylinder. After each input is depressed, the cylinder moves one position thus creating a different monoalphabetic cipher. After 26 letters of plaintext (a full rotation) the cylinder is back to its original position so we have a polyalphabetic substitution cipher of period 26.
- A single cylinder is trivial but the use of multiple cylinder is formidable.
- Figure 1.5 is a three cylinder system and the output pins of one cylinder are connected to the input pins of the next one. The LHS of figure 1.5 shows a position where the input from the operator to the first pin (plaintext letter A) is routed through three cylinders to appear at the output of the second pin (ciphertext B).
- With multiple cylinders the one furthest from the operator rotates one pin position with each operator keystroke. For every rotation of the middle cylinder the inner/slow cylinder rotates one pin position. $26 \times 26 \times 26 = 17,576$ substitution alphabets before repeating.