1. INTRODUCTION

This talk is in two halves. In the first we give an introductory overview of the 'classical' encryption techniques and look at their relative merits. This is an abridged form of [Mit2]. Then, in the second half, we look at some recent developments; notably the arrival of public key cryptography. The aim is to illustrate various applications of public key systems and to motivate the lectures of I.F. Blake and Y. Desmedt.

The development over the last 100 years of automatic means for data transmission, and more recently the dramatic evolution of electronic data processing devices, has required a parallel rapid growth of work in cryptology, the study of encryption. More and more information of a sensitive nature is both communicated and stored electronically, and so the application for cryptographic techniques are ever increasing. We will attempt to classify and describe the principle techniques for data encryption that have been proposed and used, and to indicate the chief areas of application of these different techniques.

The basic idea behind any data encryption algorithm is to define functions $f_k$, which transform messages into cryptograms, disguised forms of the original messages, under the control of secret keys, $k \in K$. Thus if we let $M$ denote the set of all possible messages, and $C$ denote the set of all possible cryptograms, we are defining a family of functions $\{f_k : k \in K\}$, where $K$ is the set of all possible keys, and $f_k(m) \in C$ for every $m \in M$. In order that decryption is always possible, every $f_k$ must be one-to-one (i.e. $f_k(m)=f_k(m')$ implies $m=m'$).

This rather abstract notion of data encryption is not necessarily a good guide to classifying the techniques actually used in cryptographic applications. In general, the idea of a special function being applied to the entire message simultaneously in order to obtain the cryptogram is rarely, if ever, used. In practice all the encryption methods in use involve dividing a message into a number of small parts (of fixed size) and encrypting each part separately, if not independently. This greatly simplifies the task of encrypting messages, particularly as messages are usually of varying lengths.

We shall assume throughout that the message parts are encrypted one at a time in the obvious order; we are thus able to use terms like: "previous parts of a message".

First we note that some cipher techniques operate on a single bit at a time, whereas others operate simultaneously on sets of bits, usually called blocks. Thus one important property relates to bit/block operation. The indivisible set of bits on which the system operates is called a character.

Secondly we observe that for some encryption techniques the encryption function which is applied to one piece of the plaintext is independent of the content of the remainder of the message. But for certain other methods, the enciphering function applied to one section of the message depends directly on the results of enciphering previous parts of the message. This property is referred to as character independence/dependence.

In some cipher systems, a message part is encrypted using precisely the same function regardless of its position within the message; in this case the cipher is said to possess **positional independence**. Other systems depend on the fact that different message parts are encrypted according to their position, and are thus **positionally dependent** ciphers.

The final characteristic property which we consider relates to the **symmetry** of the encryption function. This property, discussed more fully later, is the essential difference between conventional **symmetric** or **private key** cryptosystems and the **asymmetric** or **public key** cryptosystems. The fundamental difference is that, in an asymmetric system, encryption and decryption require different keys, and knowledge of an enciphering (or deciphering) key is not in practice sufficient to be able to deduce the corresponding deciphering (or enciphering) key.

Table 1 below illustrates how the different types of cipher system that we discuss here can be characterised in terms of these properties.

<table>
<thead>
<tr>
<th>Characteristic Property</th>
<th>Type of character</th>
<th>Character Dependence/Independence</th>
<th>Positional Dependence/Independence</th>
<th>Symmetric/Asymmetric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream Cipher</td>
<td>Bit</td>
<td>Independent</td>
<td>Dependent</td>
<td>Symmetric</td>
</tr>
<tr>
<td>Block Cipher</td>
<td>Block</td>
<td>Independent</td>
<td>Independent</td>
<td>Either</td>
</tr>
<tr>
<td>Cipher Feedback System</td>
<td>Either</td>
<td>Dependent</td>
<td>Independent</td>
<td>Symmetric</td>
</tr>
</tbody>
</table>

**Table 1 - Characterisation of Cipher Schemes**

We will give more formal definitions of the types of cipher systems and explore some of the advantages and disadvantages of each type of system. However, it is interesting to note at this point how much information is contained in the above table.

For example, it is clear that in any cipher system which has the character dependence property, error propagation will occur, i.e. if any ciphertext bits are corrupted during transmission, then a larger number of plaintext bits will be in error after decryption. Similarly, in any system which has the positional dependence property, if any message parts are lost during transmission, then all subsequent message parts will be decrypted erroneously.