CRYPTOGRAPHY - A GENERAL OVERVIEW

What is it?
Cryptography is a common, widespread and fundamental aspect of information security. It's most basic definition is that it is the practise of keeping secrets by encrypting the data, it also encompasses cryptanalysis which is the art of decrypting secret data. Both are opposite sides of the same coin. People who make cryptosystems are known as cryptographers, and those who break ciphers are known cryptanalysts. It is also important to understand the difference between codes and ciphers. Codes are words or symbols which are used to represent something ("cool" is often a code word for "looking good"), but are not meant to ensure confidentiality, whereas ciphers are designed to hide the true meaning of the message.

Cryptography takes plaintext -the unencrypted data-, transforms it into ciphertext -the encrypted data- by using a cipher -an encryption algorithm or method- and a key -a value used in conjunction with a cipher to create ciphertext. Most cryptosystems obey a fundamental idea regarding cryptosystems called *Kerchoff's Principle*. This states that the strength of a cryptosystem depends on the strength of the key, as well as the encryption algorithm.

Any encryption algorithm also needs to ensure that certain aims are met. First is *confusion*, this is where the relationship between the plaintext and the key is made complicated enough so that if an attacker has plaintext and the algorithm, they cannot make changes to the plaintext to see the resultant ciphertext and thus deduce the code. Second is *diffusion*, this means that any changes in the plaintext results in multiple changes spread throughout the ciphertext. Third is the *Claude Shannon Characteristics of a Good Cipher*, these include;

1. The amount of secrecy needed should determine the amount of work needed for the encryption and decrytption of the data.
2. The set of keys and the enciphering algorithm should be free from complexity
3. The implementation of the enciphering process should be as simple as possible
4. Any errors in the enciphering should not propagate and cause corruption of further data
5. The size of the ciphertext should be no larger than the text of the original message

Finally, any encryption algorithm should be chosen because;

- It is based upon sound mathematics
- It has been analyzed by competent experts and is sound
- It has "stood the test of time"

Data is encrypted in order to make it extremely difficult for an unauthorized person to access the data, even if they know the algorithm used and have the encrypted data. The goal of many cryptosystems is to make their encrypted data computationally infeasible to crack. Take for example a cryptosystem that used a key consisting of purely lowercase alphabetic characters and 10 characters long. That means that the attacker would have to try 10 to the power of 25 possible combinations. Assume that they could try 10,000,000 combinations a second, I will leave it as an exercise to the reader to do the maths regarding the length of time it could take to crack the key.

So we see that cryptography can provide confidentiality in it's hiding away of secret data, it can provide integrity as it can be used to detect any changes which may have happened to the data, and it can provide accountability as it can be used to verify the origin of the data. Although please bear in mind that not all cryptosystems are built to accomplish all three of these goals.

Types of Cryptosystems..
Cryptosystems are used to encipher data using a cipher, and can be broken down into a couple of broad categories;

- Symmetric encryption
- Asymmetric encryption

- Physical encryption
- Hashing encryption
- Quantum encryption

These different types sometimes can and do overlap, and some are specifically designed to meet some or all of the goals of confidentiality, integrity and accountability.

Symmetric Encryption
In this type of cryptosystem only one key is used. That means that there is only one key for both the encryption of the plaintext and the decryption of the resultant ciphertext. So if person A used a symmetric cryptosystem, with a key of X, to send an encrypted message to person B. Than person B would need to know, and use, the key of X as well as the same cryptosystem in order to decrypt the secret message. This type of encryption and decryption is very fast.

The weak point in the system is also it's strength, the key. If the key used is compromised then the entire process is compromised, so every person using the cryptosystem who wants to securely exchange data would have to keep the key secret. Now with group of a 100 people, each person would need a copy of the secret key, each of the 100 would need to securely receive their copy of the key, and then also securely use and keep it. Statistically the chances of one of 100 copies being compromised is much greater then a smaller group of 10. A similar problem is that if you want to securely exchange data with a 100 people separately, you would need to keep track of, securely keep and use, 100 different keys.

Asymmetric Encryption
This is also known as "public key" encryption. In this system each user has two keys, one private key which is kept secret, and a public key which is shared. A user can encrypt data with another person's public key to ensure that only the person with the matching private key can decrypt it. Or they could encrypt data with their private key and allow anyone with access to the public key to decrypt it.

This system allows any new users to be easily added as the same key pair is used, users can be removed easily, the key only needs to be changed when the private key has been compromised, and the distribution of keys is safe as only the public keys are distributed. The drawback to this system is the that the encryption and decryption is slower than other systems.

Physical Encryption
This method of encryption is what many of the classical encryption systems fall into. By classical I mean those systems used by the Greeks, by Caesar, etc. A general definition of these systems is that they do not encipher the data using a mathematical process.

Hashing Encryption
This encryption system uses a mathematical process to perform a calculation against the data and return a numeric or hash value. Unlike other encryption systems, hashing is a one-way system, this means that it is impossible to use the hash value to deduce the original data. But the hash value does serve as a highly effective checksum, meaning that it allows a way of seeing if the data has changed. If the checksum of data at the recipient is different to that of the originator, the data was tampered with in transit.

Quantum Encryption
This system depends on the scientific method known as *Heisenberg's Uncertainty Principle* and can only be used across fibre optic links. The scientific principle in question states that the act of observing something causes changes in that which is being observed. So when data is sent across a fibre link, the sequence and polarity of the photons is used as the key, and if the flow of photons was somehow monitored, then the sequence and polarity of the photons would be altered thus alerting the recipient of possible tampering.

Types of Ciphers..
Lets look at some of the ciphers used by cryptosystems to encode data;

- Substitution cipher
- Transposition cipher
- Steganongraphic cipher
- Block cipher
- Stream cipher

Substitution Cipher
These are ciphers that changes one character or symbol into another one. The basic way of doing this is the *Monoalphabetic Substitution Cipher*, where a single alphabet is used to make the substitution, this means that a particular character is only changed to one other particular character. This means that all "a" would be a "z", so the data of "aaa" would be "zzz". A more complicated variant of the substitution cipher is the *Polyalphabetic Substitution Cipher*, where multiple alphabets are used to encrypt the data. An example would be where the position of a character in a message would indicate that it would be replaced by a character that far ahead of it, so "aaa" becomes "bcd".

Transposition Cipher
These are ciphers which involve scrambling the letters in some way, the message is generally broken into blocks then each block is scrambled, and the letters are interchanged in some way. An example would be "attack at five", take out the spaces would give "attackatfive", split into 2 blocks of 6 would be "attack atfive". Now stack the blocks;

attack
atfive
take the 1 letter at the top, then second letter at bottom, and so on to get "attice", the remain characters are "atfavk", so the encrypted message is "attice atfavk".

Steganographic Cipher
These ciphers basically hide the secret data inside other data. The enciphered data could still look like normal data but the real message is encrypted inside it. A very basic example would be "please all gather to meet at seventeen one one", take every third word and the decrypted message is "gather at one".

Block Cipher
Ciphers like this mathematically encipher data in blocks. The plaintext data is split into blocks and then each block is enciphered to produce the total ciphertext. The are multiple ways to do this;

- ECB, Electronic Code Book is where each block is encrypted independently.
- CBC, Code Book Cipher is where the block which is to be encrypted uses the results of a mathematical process run against the previous block to help secure the encryption.
- OFB, Output Feedback Cipher is where individual blocks are not used, but the key is used to generate data the same length as the data to be encrypted, and then uses a mathematical process against the generated data to securely encrypt the plaintext.

Stream Cipher
With this cipher each bit of data is sequentially encrypted using one bit of the key, the reverse process is followed to decrypt the data. Stream ciphers can be made mathematically impossible to break by using different random keys for the encryption. One implementation of such a system is *One-Time Pads*, where each use of the encryption process uses a different key.

Well thats it, a general overview of some cryptographic principles. I hope it was interesting. It is worth getting to about cryptography as it is heavily used in our everyday lives, and the more we understand about it, the better we can chose what we use day in and day out.