Encryption

Encryption is the scrambling of data into a form that cannot be understood by unauthorised people. We Encrypt data so that it can be kept securely. Data is particularly vulnerable when it is being sent from place to place - e.g. over the internet - so the use of encryption is very important for things like ecommerce, where we want to be able to send credit card details, bank details, etc. securely without the data being stolen.

Ciphers are used in Encryption - these are complex mathematical functions which take in our plane text at one end and produce scrambled, unreadable, data at the other. Most modern encryption is Asymmetric - this means that one 'key' (actually a very large number) called the 'public key' is used to encrypt the data, and a second 'private key' is used to decrypt the data. We can tell everyone our public key, which they can then use to send data to us - as long as we keep our private key secret we can use it to unencrypt the messages we receive, but no one else will be able to.

Question 1 - Encryption has had a major impact on wars in the past. Give an example of when this was the case.

Symmetric Encryption uses the same key to both encrypt and decrypt the data. It is faster to process, but rarely is it useful if you are communicating with someone at a distance. It is used to encrypt data on a hard drive, or which you are keeping for yourself.

Question 2 - Why might you encrypt data on your own hard drive?

Generally, we never get to see our keys - they are built into our browsers, and encryption happens in the background (e.g. when we use https), but we can get stand alone applications which allow us to encrypt individual files and send a public key to other people.

Question 3 - What does https stand for? What does it do?

Question 4 - Encryption that was secure in the past may not be secure in the future. Why not?

Question 5 - The modern economy is dependent on secure encryption. If it was found that modern encryption could be broken, what would be the impact on the world?

Question 6 - Governments often try to restrict the use of encryption. Why?

Question 7 - Some governments attempt to introduce a ‘back door’ rule for encryption, meaning they can always have access to encryption used in their country. Why is this so bad for security?

Caesar Cipher

The Caesar Cipher is an old, simple, and not very secure cipher. It can be used as a way of showing how basic cryptography works. In it we replace each letter with a different one, by shifting the letters of the alphabet to the left or right by a set number of places. This shift is called the ‘key’ of the particular cipher. E.g.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

The above shows a Caesar Cipher with a shift of +20 (you could also call this a -6 shift).

If we encoded the phrase ‘SECRET MESSAGE’ it would come out as:

YKIXKZ SKYYGMK

Question 8 - Explain why the Caesar Cipher is not at all secure.