ENCRYPTION

Encryption: process of turning plaintext into scrambled ciphertext, which can only be understood if it is decrypted.

Plaintext: data in human readable form

Ciphertext: data that has been encrypted

Decryption: the process of deciphering encrypted data or messages.

Key: in cryptography is the data that has been used to encrypt and decrypt the data

Frequency Analysis: in cryptography it is the study of how often different letters or phrases are used

Substitution ciphers

Substitution Cipher: a method of encryption where one character is substituted for another to create ciphertext

- Caesar Shift: a substitution cipher where letters are shifted backwards or forwards a fixed number of places in the alphabet. Receiver would need to know the shift number to decrypt.
- Random Substitution: uses a random sequence of letters to substitute for the alphabet in the plaintext. The receiver would need the substitution sequence to Decrypt
- Keyword: substitution key starts with the keyword followed by the remaining alphabet in order (no repeats). The receiver would need to know the keyword to Decrypt

A	B	C	D	E	F	G	H	I	J	K	L	M
Q	U	I	E	T	L	Y	A	B	C	D	F	G

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	J	K	M	N	O	P	R	S	V	W	X	Z

- Polyalphabetic: uses more than one alphabet
    - Receiver would need to know all the alphabets to decrypt
    - German Enigma Machine was polyalphabetic

Transposition ciphers

Transposition Cipher: a method of encryption where the characters are rearranged to form an anagram

- Railfence Cipher: type of transposition cipher that encodes the message by splitting it over rows

D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

- Route Cipher: variation of a Railfence where the Cipher is put into a grid and read in a different a different pattern. The key is size of the grid + route over the grid.

A	B	O	R	T
T	H	E	M	I
S	S	I	O	N

Vernam Cipher

Vernam Cipher: method of encryption that uses one-time key to create Ciphertext that is mathematically impossible to decrypt without the key.

- One-time Pad: key that is only use once to encrypt & decrypt a message and then discarded
- Key is a sequence of letters as long as the plain text

Sender

1. XOR binary codes to produce a new binary code
2. Convert new binary code to a Character → Ciphertext character
3. Repeat for the every character in the plaintext

Receiver

1. Convert Ciphertext & Key into binary
2. XOR binary codes to produce new binary code
3. Convert new binary code to a character → Plaintext
4. Repeat for every character in the Ciphertext

Computational Security and Hardness

Computational Security: concept of how secure data encryption is. Secure means:

- Theoretically breakable but not using current technology in a timeframe that would be useful
- Cipher appropriate to the need to keep the secret: Military - Banking - Your Email

Computational Hardness: the degree of difficulty in cracking a cipher

Possible methods to crack codes:

- Frequency Analysis
- Identify common techniques (substitution, transposition)
- Dictionary Attacks: comparing attempts to decrypt with dictionaries to determine if anything sensible has happened
- Reverse Engineering: going back step by step
- Brute Force