ENCRYPTION CHAT STATIONS

Substitution Ciphers

Description: A substitution cipher takes a plaintext message and swaps each letter with another letter or symbol.

3 Facts / Stats / Characteristics:

1. The "key" for Caesar cipher represents how many spaces the alphabet should be rotated.
2. Double letter patterns, one letter words, and vowel placement make this method vulnerable.
3. Susceptible to brute force and frequency analysis attacks.

https://www.csfieldguide.org.nz/en/chapters/coding-encryption/substitution-ciphers/

Substitution table:

Plain	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
Cipher	**U**	**P**	**T**	**B**	**Z**	**O**	**K**	**F**	**V**			**A**	**G**	**M**	**J**			**Y**	**C**	**H**	**N**	**W**	**I**		**D**	

Examples:

https://en.wikipedia.org/wiki/Substitution_cipher

Caesar Ciphers

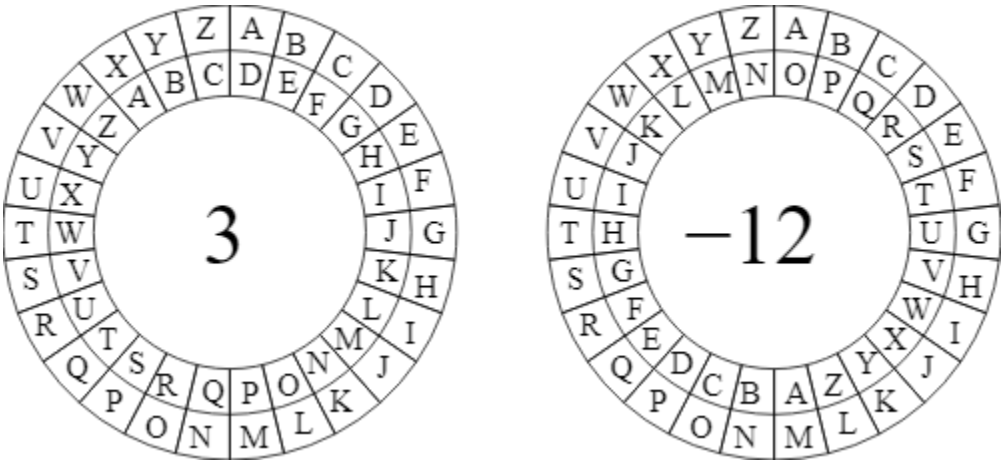

Image credited to https://cscx.org/caesar

Atbash Ciphers

https://en.wikipedia.org/wiki/Pigpen_cipher

Information about the security:

https://en.wikipedia.org/wiki/Substitution_cipher#Security

Applications:

Passing secret notes to your friends at school

Not suitable for:

Monetary transactions

Trade secrets

Classified information

Anything related to health/safety or other personal information

Language Substitution

Language substitution is a method of protecting sensitive information by communicating in a language that is unknown to eavesdroppers.

Facts / Stats / Characteristics:

1. Relies on the cipher language being secret

Example: "...United States service members during the World Wars who used their knowledge of Native American languages as a basis to transmit coded messages" (from https://en.wikipedia.org/wiki/Code_talker).

Applications:

Informal conversations

Alien invasions

Counterintelligence

Limitations:

After the success of code talkers in World War II, it's much more difficult to pull this off in high profile scenarios.

https://fronterasdesk.org/content/1005301/navajo-code-talkers-miracle-ended-world-war-ii

https://www.nationalww2museum.org/war/articles/american-indian-code-talkers

Symmetric Encryption

Symmetric encryption uses a secret shared between two parties as a key to encrypt data. It is "symmetric" because each person in the communication uses the key to encode and decode messages.

https://www.csfieldguide.org.nz/en/chapters/coding-encryption/storing-passwords-securely/

Examples:

https://en.wikipedia.org/wiki/One-time_pad

Examples of popular symmetric-key algorithms include Twofish, Serpent, AES (Rijndael), Camellia, Salsa20, ChaCha20, Blowfish, CAST5, Kuznyechik, RC4, DES, 3DES, Skipjack, Safer, and IDEA.

(from https://en.wikipedia.org/wiki/Symmetric-key_algorithm#Implementations)

Applications:

Digital signatures

Data Hashing

Communication

Limitations:

- Protecting a single shared secret is difficult because of hackers and the way information is proliferated on the internet.
- Breaking symmetric encryption receives a lot of attention and interest from hackers. There are many tools and techniques available to assist in "discovering" the shared secret.
- Establishing a shared secret requires a pre-existing, safe way to communicate.

Asymmetric Encryption (aka Public-key cryptography)

Asymmetric encryption uses a combination of private and public keys from two parties to encrypt data. It is "asymmetric" because each person in the communication uses a different key to encode and decode messages.

https://www.csfieldguide.org.nz/en/chapters/coding-encryption/the-key-distribution-problem/

Facts / Stats / Characteristics:

1. Anyone can use the public key to encrypt.
2. Only the private key holder can decrypt an encoded message.

Examples:

Diffie-Hellman Key Exchange

RSA encryption algorithm

Elliptic curve cryptography

Applications:

- Internet security. Almost all safety and security on the internet is implemented with public-key cryptography.
- Robust digital signatures
- Digital currency

Limitations:

- Can be challenging to understand
- Keeping private keys safe can be difficult