Università della Svizzera italiana

C&QI Cryptography & Quantum Information

Ciphers and Attacks

Arne Hansen and Prof Stefan Wolf
Cryptography and Quantum Information, USI Lugano

Ways of Hiding Information

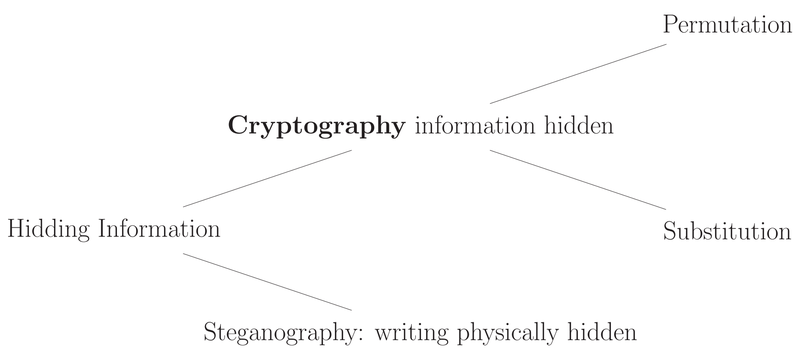
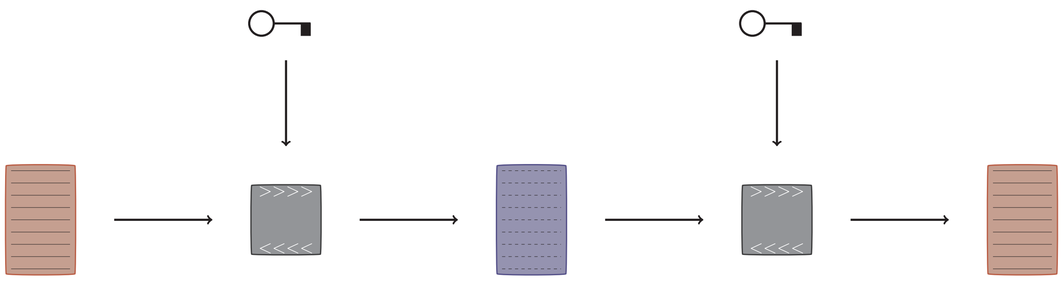


Figure : Categories of Secrecy

Cryptography hiding content of a message without hiding the writing itself.
Steganography physically hiding the message (invisible ink, . . .)

The Scheme of Cryptography



The plaintext is together with a key are given to an encryption algorithm generating the ciphertext. The ciphertext is then sent to another party. With the right key the message can be deciphered again.

Scytale: a transposition cipher

The message “Help me, I am under attack” is written on the scytale in rows

H	E	L	P	M
E	I	A	M	U
N	D	E	R	A
T	T	A	C	K

After unwinding the band it becomes scrambled to

`HENTEIDTLAEAPMRCMUAK`

The Caesar Shift Cipher

The simplest substitution cipher is the Caesar Cipher. Caesar shifted all the letters down the alphabet by a fixed step, say for instance 3 letters. The plaintext and ciphertext alphabet are associated as follows

Plaintext: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
Cipher: `XYZABCDEFGHIJKLMNOPQRSTUVW`

An example encryption would be

```
Some important message.
PLJB FJMLOQXKQ JBPPXDB.
```

Navajo Code: an unbroken ‘linguistic’ code

During WWII machine ciphers have been common among all parties. A major drawback was the time effort to encode and decode. In critical situations that required fast communication encryption was thus dropped revealing the content directly to the enemy. Therefore in 1942 Philip Johnston, a US American engineer, suggested to translate message to the tribal language of the Navajo before transmission. As its grammar and vocabulary was not related to neither European nor Asiatic languages it served as a very secure cipher. Therefore Navajos were recruited as translators and cryptographers. While machine ciphers were frequently broken, the Navajo language was never.

Frequency Analysis

The One-Time Pad

Enigma: a first machine cipher

Recommended Encryption Tools

GNU Privacy Guard (GnPG): implementation of OpenPGP