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

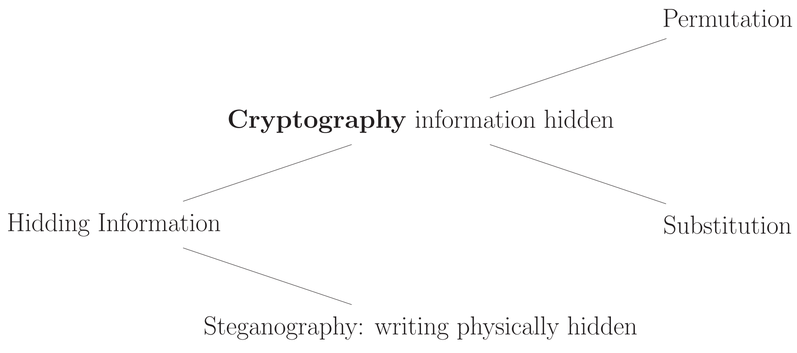
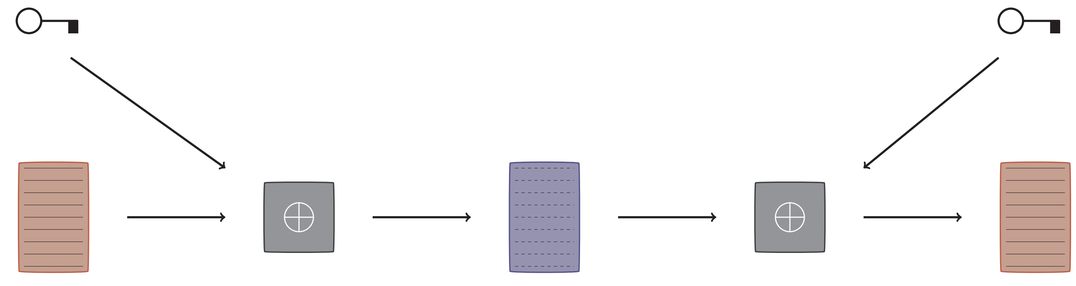


Figure : Categories of Secrecy

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

The Scheme of Cryptography



A first player, usually called Alice, encrypts the plaintext according to the encryption algorithm using her key. The ciphertext Alice generated is then sent to another party, often called Bob. With his key he can execute the decryption algorithm in order to obtain the plaintext again.
Security What does it mean for a cipher to be secure? The notion of security depends on the abalities we imagine an adversary has to attack the cipher. The adversary, often referred to as Eve, can at least read the ciphertext, i.e. tap the wire between Alice and Bob. Usually Eve also knows the encryption and decryption algorithms. Obviously Alice and Bob have to keep their key secret. If Eve's knowledge of the algorithms and the ciphertext suffices to retrieve the plaintext, the cipher is insecure. Otherwise Alice and Bob can communicate secretely.
Authenticity What if Eve doesn't merely read the ciphertext but also changes it? Or sends something to Bob, claiming to be Alice? This would be a scenario with a stronger adversary. These considerations lead for instance to *digital signatures*.

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 scytale is thus a permutation cipher.

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.`

Frequency Analysis

The letters of the alphabet do not occur with the same frequency. In English the letter "e" is the most common and occurs a lot more often than for instance "z". So if one knows in what language a plaintext was written, one can decrypt the ciphertext from a monoalphabetic substitution cipher without knowing the substitution scheme. One merely has to count the number of occurences of any letter of the alphabet, compare this with the frequencies of letters of the given language and match corresponding letters. This works better the longer the cipher text is. (Actually if the ciphertext is very short, the cipher might become a one-time pad which is really secure).

The One-Time Pad

How could we get a substitution cipher with proper security? The issue of most substitution ciphers is their redundancy. For example the letter "e" might always be substituted by "m". This clearly allows frequency attacks as the number of occurences of "e" is just shifted to "m". In order to get rid of any redundancy or other structures that might be helpful to break the cipher the one-time pad uses an entirely random key that is just as long as the message itself. A binary example as it occurs in any computer is then

Text	`Ciao`
Plaintext	`01000011 01101001 01100001 01101111`
	$\oplus$
Key	`10011011 11110011 10011100 11011011`
	gives
Ciphertext	`11011000 10011010 11111101 10110100`

So adding the key (i.e. applying the XOR (either . . . or . . .) operation) makes the ciphertext to look completely random too. In other words: (something completely random) $\oplus$ (something with structure) = (something completely random). As the ciphertext looks random to Eve she has no means to decipher it. Thus the one-time pad is properly secure. As the name already suggest: never ever use it even twice. This would introduce structure and therefore turn the cipher insecure.
Why isn't the OTP used all over the place if it is completely secure? Well, you need to distribute a lot of keys secretely. This is very inconvenient. Current ciphers provide a very good level of security as the resources needed to break them exceed the computational power of recent computer by far.

Enigma: a first machine cipher