Cipher definition

A cryptosystem (cipher) can be defined as a quintuple (P, C, K, E, D) where: - P is the set of plain texts - C is the set of cipher texts - K is the set of keys - $E : k \times P \rightarrow C$ is the encryption function. - $D : k \times C \rightarrow P$ is the decryption function. ## Symmetric Given $x \in P, y \in C, k \in K$, $E_k(x)$ and $D_k(y)$ mean $E(k, x)$ and $D(k, y)$ i.e. encryption and decryption of plain text x and decryption of cipher text y under the key k. [[caesar.png]]

It is required that $D_k(E_k(x)) = x$ i.e. decryption of the cipher text with the right key gives back the original plain text message. It is also required that computing the original plain text x should be unfeasible. ## Kerckhoffs' principle A cipher should remain secure even if the algorithm becomes public. ### Kerchoffs' rules - The system should be unbreakable, atleast in practice (computationally impossible). - The design of a system should not require secrecy, meaning that if the inner workings of a system are known, the system should still work. ## Shift cipher $P = C = K = Z_{26}$ where Z_{26} means all integer numbers modulo 26. ## Attacks on shift ciphers ### Bruteforce Trying all possible keys, in this case 26. # Group A group $< G, * >$ is a set G with a binary operation $*$ on G such that: - $*$ is associative, meaning $(x * y) * z = x * (y * z)$, $\forall x, y, z \in < G, * >$ - $\exists e \in G$ such that $a * e = e * a = a$, $\forall a \in G$. This element is knows as **identity element**. - $\forall a \in G$, $\exists b \in G$ such that $a * b = e$. That element b is know as the **inverse** of a with respect to $*$. ## Abelian group A group that is commutative with an additive operation e.g. $< Z, + >$ is an abelian group. # Substitution cipher $P = C = Z_{26}$, $K = \{p | p$ is a permutation of $0, \ldots, 25\}$ Also, $E_k(x) = p(x)$ and $D_k(y) = p^{-1}(y)$ The two properties still hold: - $D_p(y) = D_p(E_p(x)) = D_p(p(x)) = p^{-1}(p(x)) = x$ - A brute force attack is unfeasible because there are 26! permutations because the key is a permutation of the alphabet. ## Breaking substitution ciphers - This type of cipher is a mono alphabetic cipher, this means that every letter is mapped to only one other letter (e.g. the letter A will always be mapped to F). This can lead to frequency based attack, i.e. an attacker will try to recreate the plain text computing the frequencies of the letters and trying to "guess" the original one. (see example in slides) # Poly alphabetic ciphers The same plain symbol (the letter) is not always mapped to the same cipher symbol. ## Vigenére cipher The plain text is split into blocks of length m and the key (that has the same length m) is repeated as long as the message and is used to encrypt each block. [[vigenere.png]] Formally, $P = C = K = Z_{26}^m$ where Z_{26}^m is the Cartesian product $Z_{26} \times Z_{26} \ldots Z_{26}$ m times $E_{k1,\ldots,km}(x_1, \ldots, x_m) = ((x_1 + k_1)\%26, \ldots (x_m + k_m)\%26)$ This means that the encryption is done by adding the value of the key (positional number of letter) with the original one, as shown in the previous image. Viceversa, the decryption is done in the same way. $D_{k1,\ldots,km}(y_1, \ldots, y_m) = ((y_1 - k_1)\%26, \ldots (y_m - k_m)\%26)$ The number of possible keys is 26^m, this represents all possible sequences of letters with a length of m. This means that the brute force attack for big keys is unfeasible.