|  |  |  |  |
| --- | --- | --- | --- |
|  | **Atbash Cipher** | **Caesar Cipher**  Shift Cipher | **Transposition Cipher**  Columnar Transposition |
| **Who** |  | Julius Caesar |  |
| **When** | Early B.C | 100 B.C | 1900 BC |
| **What** | Atbash cipher is a substitution cipher with just one specific key. It was originally used to encode the Hebrew alphabets but it can be modified to encode any alphabet. | of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. | reorder units of plaintext (typically characters or groups of characters) according to a regular system to produce a ciphertext which is a permutation of the plaintext. |
| **Properties** | * Substitution * Letter Reversal   Picture  Picture | * Substitution * Shift according to key count | * Scrambled Position * Row Length according to Key * Encrypted message grouped by 5 * Read in Columns |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Polyalphabetic Cipher**  Vigenère | **Vernam** | **RSA** |
| **Who** | Leon Battista Alberti | Gilbert Sanford Vernam | Ronald Rivest, Adi Shamir, Leonard Adleman |
| **When** | 1467 | 1917 | 1977 |
| **What** | using a series of interwoven Caesar ciphers, based on the letters of a keyword. It employs a form of polyalphabetic substitution. The original plaintext structure is somewhat concealed in the ciphertext by using several different monoalphabetic substitution ciphers rather than just one; the code key specifies which particular substitution is to be employed for encrypting each plaintext symbol. | a symmetrical stream cipher in which the plaintext is combined with a random or pseudorandom stream of data (the "keystream") of the same length, to generate the ciphertext, using the Boolean "exclusive or" (XOR) function. | In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers. |
| **Properties** | * Substitution | * Substitution * One Time Pad * XOR | * Public & Private Key * 2 Prime Numbers ( ***p*** & ***q*** ) * Modulus ***n*** = ***pq*** * Totient ***phi*** = (***p*** – 1) \* (***q*** – 1) * Encryption Key ***e***  = 1 < ***e*** < ***phi*** = ***e*** coprime ***n*** * Public Key = (***e*** , ***n*** ) * Decryption Key ***d*** = ***e-1***  % ***phi*** * Private Key = ( ***d*** ) |