**VARIOUS CIPHERS**

1. *Public-Key Crytography*

This is one of the most widely used types of codes or cipher. It is modern and is made of two keys – the private and the public key. The public key is a large number everyone can get. The private key is made of two numbers (apart from 1 and the number itself). These two numbers are multiplied together and can produce the public key. For example, the public key is 1764, the private key can be 36 and 49 (36×49=1764).

It is very secure and is used in emails, bank access details etc. **Without the private key, the code cannot be deciphered**. It is very difficult to find out the divisors of large numbers. RSA Company ever offered money to people who could find 1 divisors of the numbers they gave.

### *Transposition Cipher*

This particular cipher was used during American Civil War and World War I to communicate sensitive messages. **The letters of the alphabet are rearranged based on pre-determined key or rule.** It could be that all the words in the message are written backwards, or every pair of letters is swapped. If the rearrangement rule is complex, it might seem very difficult to decipher, however, with modern algorithms on the computer, it can be easily deciphered. For example: “the yellow car belongs to him” can become “eht wolley rac sgnoleb ot mih” when written backwards.

### *Book Cipher*

This particular cipher involves the use of some key, essentially in a book. Both the parties should have the same book and the same edition to successfully decipher the code.**Locations in the book are used to replace the plain text of the message.**The ease of decoding depends on the how well the key has been chosen. Also the book should be inconspicuous and of the genre which is similar to the type of messages required to be sent. The Book Cipher has been widely used in various novels, TV series and movies. In the novel The Valley of Fear, Sherlock Holmes has deciphered a message with the book cipher.

### *Playfair Cipher*

Here we come to the last one on the list of types of codes and ciphers. The Playfair cipher is also known as the Playfair Square. It was the first literal digraph substitution cipher and involves the manual symmetric encryption technique. It was invented by Charles Wheatstone in 1854, but is named after the person who promoted its use. **In this type of cipher, pairs of letters are encrypted instead of single letters.**Thus it is harder to decipher. It creates 600 possible digraphs as compared to 26 monographs. This cipher also has been used in crossword, novels, movies and audio books. In the film National Treasure: Book of Secrets, the Playfair cipher is used to encode a treasure hunt clue.

### *Pigpen Cipher*

This is also referred to as Tic-Tac-Toe Cipher, and is fairly simple substitution cipher. **The letters of the alphabet are replaced by fragments of a geometrical grid.**It is very simple and hence has been used in children’s books of secret writing as well. Although its origin cannot be ascertained, it goes back to the 18thcentury. The grid and the dots are the core elements of the cipher. The alphabets are arranged in two grids, followed by two Xs. It has been used in various novels –The Lost Symbol by Dan Brown, games like Assasin’s Creed II, TV series – Sherlock, etc.

### *Scytale*

This is an old form of cryptography, which was used by ancient Greeks and Spartans during military campaigns.**It falls under the transposition cipher and involves a parchment with a message wrapped around a cylinder.** The recipient of the message then winds the parchment on a cylinder of the same size to decipher the message. It is fast and not prone to mistakes, however, it is easy to decode. It is said that it was used more of authentication than for encryption.

DISADVANTAGES OF CIPHERS

Symmetric Ciphers

Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally. Cannot provide digital signatures that cannot be repudiated.

Asymmetric Ciphers

A disadvantage of using public-key cryptography for encryption is speed: there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.