**Lab1**

**Your Task:**

1. Learn the basics of encryption algorithms.
2. Encrypt the specified text "Surname Name Patronymic" using ciphers: Caesar, Vigenère, Playfair, the method of transposition.

**Sample Solution**

* **Caesar cipher -**  is one of the simplest and most widely known [encryption](http://en.wikipedia.org/wiki/Encryption) techniques. It is a type of [substitution cipher](http://en.wikipedia.org/wiki/Substitution_cipher) in which each letter in the [plaintext](http://en.wikipedia.org/wiki/Plaintext) is replaced by a letter some fixed number of positions down the [alphabet](http://en.wikipedia.org/wiki/Alphabet). Alphabet is cyclical, that is, after the Z should be A. Caesar is replaced by the letter that is separated from the original three. These codes are revealed extremely simply without any knowledge of the key values​​: it is enough to know only the encryption algorithm, and the key can be chosen simple search (the so-called power attack).

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Z=3 | | | | | | | | | | | | |
| Text | F | U | N | D | A | M | E | N | T | А | L | S |
| Cipher | I | X | Q | G | D | P | H | Q | W | D | O | V |
| Z=3 | | | | | | | | | | | | |
|  | O | F |  |  |  |  |  |  |  |  |  |  |
|  | R | I |  |  |  |  |  |  |  |  |  |  |
| Z=5 | | | | | | | | | | | | |
| Text | I | N | F | O | R | M | A | T | I | O | N |  |
| Cipher | N | S | K | T | W | R | F | Y | N | T | S |  |
| Z=2 | | | | | | | | | | | | |
| Text | S | E | C | U | R | I | T | Y |  |  |  |  |
| Cipher | U | G | E | W | T | K | V | A |  |  |  |  |

Surname Name Patronymic with shift 3 -> Vxuqdph Qdph Sdwurqbplf

* The **Vigenère cipher** is a method of [encrypting](http://en.wikipedia.org/wiki/Encryption) [alphabetic](http://en.wikipedia.org/wiki/Alphabet) text by using a series of different [Caesar ciphers](http://en.wikipedia.org/wiki/Caesar_cipher) based on the letters of a keyword. It is a simple form of [polyalphabetic substitution](http://en.wikipedia.org/wiki/Polyalphabetic_cipher). For encryption the text install the key, which is a word or set of letters. Next, from the full matrix without the letter E is chosen submatrix encryption. It includes the first row and the rows, which are the initial letters of a sequence of letters key. The encryption process is as follows: to obtain the ciphertext (ciphertext), we take the first character of the plaintext as a string pointer in Table Vigenere, and standing beneath the letter - as a column. At the intersection of the pair of tables write out the character ciphertext. Then repeat this process for all the remaining characters.

Text: FUNDAMENTALS OF INFORMATION SECURITY

The code word: XIAOMI

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 1 | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| 2 | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| 3 | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 4 | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| 5 | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| 6 | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |

Text: FUNDAMENTALS OF INFORMATION SECURITY

Key word: XIAOMI

Cryptogram: CCNRMUBVTOXA LN IBRWOUAHUWK AEQGZFBY

Text: Surname Name Patronymic

Key word: XIAOMI

Cryptogram: Pcrbmub Vaaq Xxbrczgjqc

* The **Playfair cipher** or **Playfair square** is a manual [symmetric](http://en.wikipedia.org/wiki/Symmetric_key_algorithm) [encryption](http://en.wikipedia.org/wiki/Encryption) technique and was the first literal [digraph substitution](http://en.wikipedia.org/wiki/Polygraphic_substitution) cipher.The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.

To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.

To encrypt a message, one would break the message into digraphs (groups of 2 letters) such that, for example, "HelloWorld" becomes "HE LL OW OR LD", and map them out on the key table. If needed, append a "Z" to complete the final digraph. The two letters of the digraph are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

1. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any uncommon monograph will do.
2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same **row** as the first letter of the plaintext pair.

* Cipher permutation (transposition) with fixed d (d-block of group of symbols). This is a block method. The text is divided into blocks and permutation of the symbols is made in each of them. Commutation rules are given by secret key. If there is insufficient letters for the full block of text you can add symbols.

Text: FUNDAMENTALS OF INFORMATION SECURITY

Key: XIAOMI

Cipher text: BZKFOXFLRMSYMEMHEMTAMRAMLTFDWPMQUO

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| X | I | А | O | M |
| B | C | D | E | F |
| G | H | K | L | N |
| P | Q | R | S | T |
| U | V | W | Y | Z |

Text: Surname Name Patronymic

Key: XIAOMI

Cipher text: PY TK OX FL OX BS MR SA LZ XA BI