Криптографски алгоритми

# Шифър на Цезар

## Криптиране

1. Определяне на множеството от разрешени символи M = {m1, m2, …, mn}.
2. Проверка дали явния текст съдържа символи, които не са част от M.
3. Преобразуване на явния текст в криптограма, използвайки формулата , където:
   * k1 – коеф. На преобразуване; k1 = 1;
   * k2 – коеф. На изместване; k2 =3;
   * i – пореден номер на символа (в M), който бива заместван;
   * j – пореден номер на символа в М, с който се извършва заместването;
   * n - |M| (брой на разрешени символи в системата).

## Декриптиране

1. За получаване на явния текст от криптограмата се използва същата формула като при криптирането само че със знак : .

# Директно (пряко, просто) заместване

## Криптиране

1. Определяне на множеството от разрешени символи M = {m1, m2, …, mn}.
2. Определяне на множеството от символи за заместване N = {n1, n2, …, nn}.
3. Определяна на функционална зависимост , чрез която всеки символ от M се замества със съответния му символ или множество от символи в N.
4. Проверка дали явния текст съдържа символи, които не са част от M.
5. Извършване на заместването за всеки символ от явния текст, използвайки , до получаване на криптограмата.

## Декриптиране

1. Заместване на всеки от символите от криптограмата, използвайки обратната функция на , до получаване на явния текст.

# Многоазбучно заместване

## Криптиране

1. Дефиниране на крайно подредено множеството от разрешени символи M = {m1, m2, …, mn}.
2. Определяне на криптографски ключ, чиито елементи се избират от M.
3. Проверка дали явния текст съдържа символи, които не са част от M.
4. Заместване на всеки символ от съобщението в явен вид (P = p1, p2, …, pq) със символ от M, който се определя с помощта на ключа (K = k1, k2, …, km).
5. Шифроването се извършва по следната схема:

където – пореден номер на символа в M, – брой на разрешените символи (|M|).

1. Ключът K е с по-малка дължина от съобщението и затова се използва циклично. По този начин един символ от явния текст се шифрова с различни символи от M, откъдето произлиза и името на метода.

## Декриптиране

1. При декриптиране се извършва обратната процедура. Всеки символ от криптограмата се замества със символ от M по следната схема:

Така се получава оригиналното съобщение в явен вид.

# Многоазбучно заместване

## Криптиране

1. Определяне на множеството от разрешени символи M = {m1, m2, …, mn}.
2. Изграждане на квадратна матрица A с размерност n x n, където n е броят на елементите от M. A се изгражда чрез едносимволно преместване наляво на елементите от M при формирането на всеки следващ ред.
3. Определяне на криптографски ключ, чиито елементи се избират от M (K = k1, k2, …, kp).
4. Съставяне на производна матрица по следния начин:

От основната матрица А се взема първия ред и онези редове, започващи със символите от ключа, взети в същата последователност.

, като k1 = mi, k2 = mj, …, kp = mn-1.

1. Съобщението в явен вид P = p1, p2, …, pq се обработва посимволно, като за всеки символ се търси мястото му в първия ред от матрицата , което определя номера на търсения стълб, а сечението на този стълб с реда, започващ с ki определя ci (символа, с който ще се шифрова pI).
2. Криптографският ключ се използва циклично до получаване на резултатната криптограма C = c1, c2, …, cq.

## Декриптиране

1. Използва се същата производна матрица , определена от криптографския ключ.
2. На всеки елемент от криптограмата C се съпоставя съответстващия му елемент от криптографския ключ: (ключът отново се използва циклично).
3. Редът в матрицата се определя от елемента ki.
4. В този ред се търси и намира символът ci, който определя номера на стълба.
5. Сечението на дефинирания по този начин стълб с първия ред на матрицата определя символа pi.