Методы шифрования

Оглавление

- Шифрование
- Методы и алгоритмы шифрования
  - Метод замены или подстановки
  - Метод перестановки
  - Метод гаммирования
  - Метод сложного математического преобразования
  - Комбинированные методы

Шифрование

Шифрование - это способ изменения сообщения или другого документа, обеспечивающее искажение (сокрытие) его содержимого.

Шифрование используется ровно с того момента, когда появилась первая личная или секретная информация, т.е. доступ к которой должен быть ограничен.

Тому лицу, что использует шифровку, важна ее устойчивость к дешифрованию или криптостойкость. Повысить криптостойкость можно путем использования более современных и сложных типов шифрования информации.

Методы и алгоритмы шифрования

Среди множества разнообразнейших способов шифрования можно выделить следующие основные методы:

- Метод замены или подстановки;
- Метод перестановки;
- Метод гаммирования;
- Метод сложного математического преобразования;
- Комбинированные методы;

Метод замены или подстановки

В этом наиболее простом методе символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов.

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

Рис.1: таблица Виженера

Метод перестановки

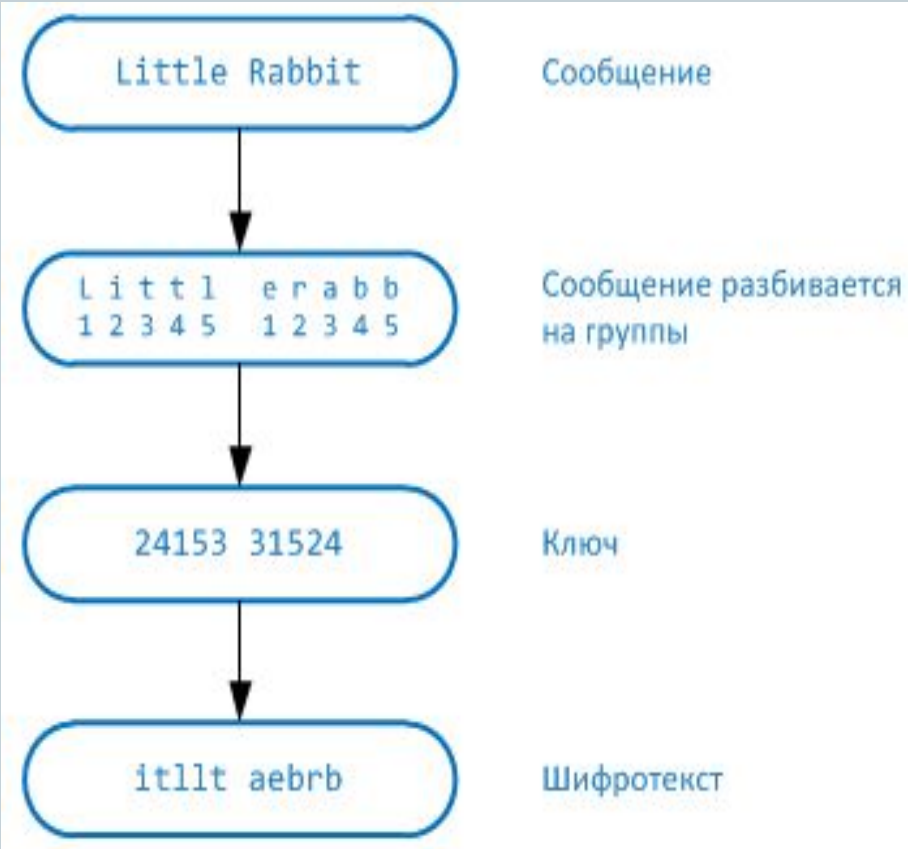

Рис.2: алгоритм метода перестановки

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов

Метод гаммирования

В методе гаммирования шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите. Если в исходном алфавите, например, 33 символа, то сложение производится по модулю 33. Такой процесс сложения исходного текста и ключа называется в криптографии наложением гаммы.

Исходный текст: *Гаммирование*

Исходный текст в шестнадцатеричном виде:

83 A0 AC AC A8 E0 AE A2 A0 AD A8 A5

Гамма (Ключ): *Весна (82 A5 E1 AD A0)*

Гаммирование

Исх. биты	1000	0011	1010	0000	1010	1100
Гамма	1000	0010	1010	0101	1110	0001
Результат	0000	0001	0000	0101	0100	1101

Исх. биты	1010	1100	1010	1000	1110	0000
Гамма	1010	1101	1010	0000	1000	0010
Результат	0000	0001	0000	1000	0110	0010

Исх. биты	1010	1110	1010	0010	1010	0000
Гамма	1010	0101	1110	0001	1010	1101
Результат	0000	1011	0100	0011	0000	1101

Исх. биты	1010	1101	1010	1000	1010	0101
Гамма	1000	0010	1010	0101	1110	0001
Результат	0010	1111	0000	1101	0100	0101

Закодированный текст в шестнадцатеричном виде:

01 05 4D 01 08 62 0B 43 0D 2F 0D 45

Метод сложного математического преобразования

Метод основан на свойствах простых чисел (причем очень больших). Простыми называются такие числа, которые не имеют делителей, кроме самих себя и единицы. Широко применяется в интернете. Сам алгоритм можно взломать лишь путем полного перебора.

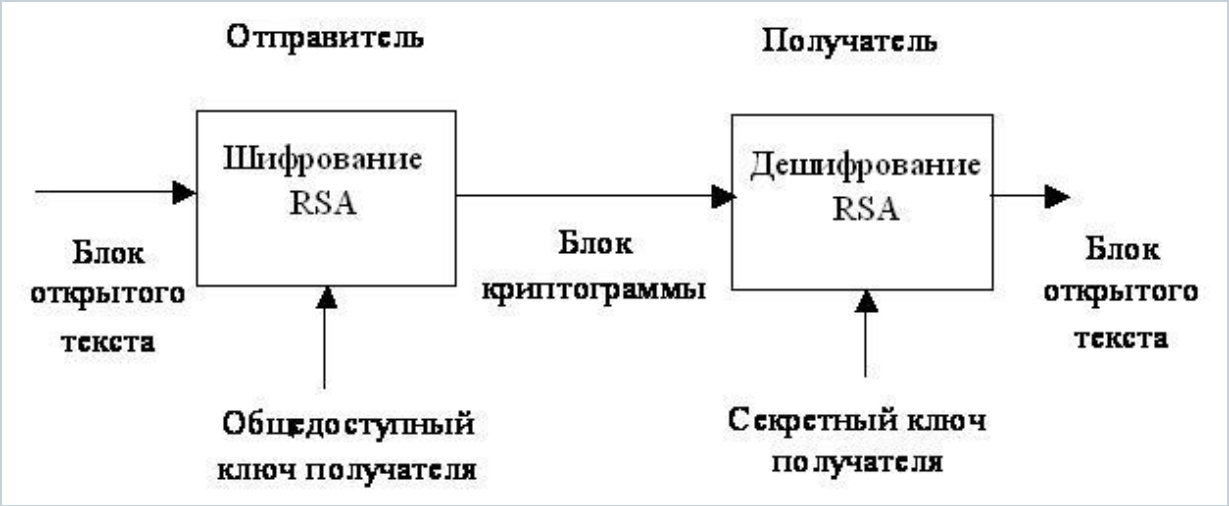

Рис.3: алгоритм математического шифрования RSA

Комбинированные методы

Одним из важнейших требований, предъявляемых к системе шифрования, является ее высокая стойкость. Однако повышение стойкости любого метода шифрования приводит, как правило, к существенному усложнению самого процесса шифрования и увеличению затрат ресурсов.

Типичным примером комбинированного шифра является национальный стандарт США криптографического закрытия данных (DES).