Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Отчёт по лабораторной работе №2

По дисциплине «Методы защиты информации»
По теме «Симметричная криптография. СТБ 34.101.31-2011»

Выполнил:
студент гр. 653501
М.Л.Спасёнов
Проверил:
В.С.Артемьев

Минск 2019

Введение

СТБ 34.101.31-2011 - государственный стандарт симметричного шифрования и контроля целостности Республики Беларусь

Настоящий стандарт определяет семейство криптографических алгоритмов, предназначенных для обеспечения конфиденциальности и контроля целостности данных. Обрабатываемыми данными являются двоичные слова (сообщения). Криптографические алгоритмы стандарта построены на основе базовых алгоритмов шифрования блока данных.
Базовые алгоритмы шифрования блока данных:

- алгоритмы шифрования в режиме простой замены;
- алгоритмы шифрования в режиме сцепления блоков;
- алгоритмы шифрования в режиме гаммирования с обратной связью;
- алгоритмы шифрования в режиме счётчика;
- алгоритм выработки имитовставки ;
- алгоритмы одновременного шифрования и имитозащиты данных;
- алгоритмы одновременного шифрования и имитозащиты ключей;
- алгоритм хэширования;

Алгоритм

Входными данными алгоритмов зашифрования и расшифрования являются блок 128b и ключ 256b.

Выходными данными является блок 128b результат зашифрования или расшифрования.

Слово X записывается в виде $X = X1 \parallel X2 \parallel X3 \parallel X4$, где $Xi \in \{0, 1\}_{32}$ Ключ θ записывается в виде $\theta = {}_1 \parallel {}_2 \parallel \ldots \parallel {}_8$, ${}_i \in \{0, 1\}_{32}$, и определяются тактовые ключи $K_1 = {}_1$, $K_2 = {}_2, \ldots, K_8 = {}_8$, $K_9 = {}_1$, $K_{10} = {}_2, \ldots, K_{56} = {}_8$.

Вспомогательные преобразования

Подстановка H. H $\{0,1\}^8$ -> $\{0,1\}^8$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	B1	94	BA	C8	0A	08	F5	3B	36	6D	00	8E	58	4A	5D	E4
1	85	04	FA	9D	1B	B6	C7	AC	25	2E	72	C2	02	FD	CE	0D
2	5B	E3	D6	12	17	B9	61	81	FE	67	86	AD	71	6B	89	0B
3	5C	B0	C0	FF	33	C3	56	B8	35	C4	05	AE	D8	E0	7F	99
4	E1	2B	DC	1A	E2	82	57	EC	70	3F	CC	F0	95	EE	8D	F1
5	C1	AB	76	38	9F	E6	78	CA	F7	C6	F8	60	D5	BB	9C	4F
6	F3	3C	65	7B	63	7C	30	6A	DD	4E	A7	79	9E	B2	3D	31
7	3E	98	B5	6E	27	D3	BC	CF	59	1E	18	1F	4C	5A	B7	93
8	E9	DE	E7	2C	8F	0C	0F	A6	2D	DB	49	F4	6F	73	96	47
9	06	07	53	16	ED	24	7A	37	39	CB	A3	83	03	A9	8B	F6
A	92	BD	9B	1C	E5	D1	41	01	54	45	FB	C9	5E	4D	0E	F2
B	68	20	80	AA	22	7D	64	2F	26	87	F9	34	90	40	55	11
C	BE	32	97	13	43	FC	9A	48	A0	2A	88	5F	19	4B	09	A1
D	7E	CD	A4	D0	15	44	AF	8C	A5	84	50	BF	66	D2	E8	8A
E	A2	D7	46	52	42	A8	DF	B3	69	74	C5	51	EB	23	29	21
F	D4	EF	D9	B4	3A	62	28	75	91	14	10	EA	77	6C	DA	1D

Преобразования G (r = 5, 13, 21). По формуле 1.

$$G_r(u) = \mathtt{RotHi}^r\,(H(u_1) \parallel H(u_2) \parallel H(u_3) \parallel H(u_4))\,.$$

фор. 1

Где RotH i^r - циклический сдвиг влево на r бит.

H(u) - операция замены 8-битной входной строки подстановкой из таблицы 1

Алгоритм зашифрования

1) Установить a <- X_1 ,b <- X_2 ,c <- X_3 ,d <- X_4
2) Для i = 1..8, выполнить(см рисунок 1)

$$
\begin{aligned}
&1)\ b \leftarrow b \oplus G_5(a \boxplus K_{7i-6});\\
&2)\ c \leftarrow c \oplus G_{21}(d \boxplus K_{7i-5});\\
&3)\ a \leftarrow a \boxminus G_{13}(b \boxplus K_{7i-4});\\
&4)\ e \leftarrow G_{21}(b \boxplus c \boxplus K_{7i-3}) \oplus \langle i \rangle_{32};\\
&5)\ b \leftarrow b \boxplus e;\\
&6)\ c \leftarrow c \boxminus e;\\
&7)\ d \leftarrow d \boxplus G_{13}(c \boxplus K_{7i-2});\\
&8)\ b \leftarrow b \oplus G_{21}(a \boxplus K_{7i-1});\\
&9)\ c \leftarrow c \oplus G_5(d \boxplus K_{7i});\\
&10)\ a \leftrightarrow b;\\
&11)\ c \leftrightarrow d;\\
&12)\ b \leftrightarrow c.
\end{aligned}
$$

,

рис.1

где $\boxplus$ и $\boxminus$ - операции сложения и вычитания по модулю 2^{32}

$\oplus$– XOR ,

$\leftrightarrow$– $SWAP$

3) Установить Y <- a || b || c || d
4) Возвратить Y

Алгоритм расшифрования

Для расшифрования применяют следующие шаги:

1) Установить a <- X_1 ,b <- X_2 ,c <- X_3 ,d <- X_4
2) Для i=1 .. 8, выполнить(см. рис. 2)

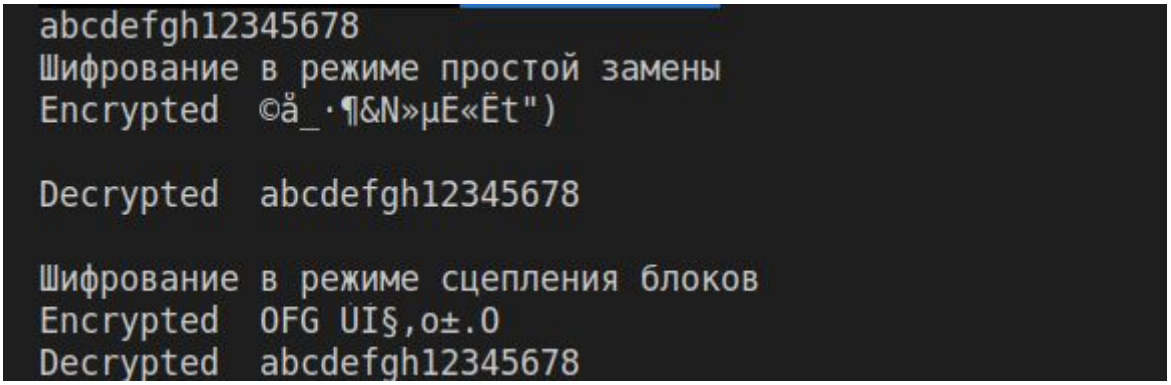
$$
\begin{aligned}
&1)\ b \leftarrow b \oplus G_5(a \boxplus K_{7i});\\
&2)\ c \leftarrow c \oplus G_{21}(d \boxplus K_{7i-1});\\
&3)\ a \leftarrow a \boxminus G_{13}(b \boxplus K_{7i-2});\\
&4)\ e \leftarrow G_{21}(b \boxplus c \boxplus K_{7i-3}) \oplus \langle i \rangle_{32};\\
&5)\ b \leftarrow b \boxplus e;\\
&6)\ c \leftarrow c \boxminus e;\\
&7)\ d \leftarrow d \boxplus G_{13}(c \boxplus K_{7i-4});\\
&8)\ b \leftarrow b \oplus G_{21}(a \boxplus K_{7i-5});\\
&9)\ c \leftarrow c \oplus G_5(d \boxplus K_{7i-6});\\
&10)\ a \leftrightarrow b;\\
&11)\ c \leftrightarrow d;\\
&12)\ a \leftrightarrow d.
\end{aligned}
$$

рис. 2

3) Установить Y <- a || b || c || d
4) Возвратить Y

Ход работы программы

На вход подается строка, которую требуется зашифровать.
На выходе строка в виде зашифрованного сообщения.



Вывод

Алгоритм СТБ 34.101.31-2011, на деле, оказался достаточно простым в разработке, и имеет различные группы для шифрования и контроля целостности.