Georgian Technical University

Informatics and Control Systems Faculty

New Tweakable Block Cipher

Levan Julakidze
PHD in Informatics

Zurab Kochladze
TSU Associated Professor

Tinatin Kaishauri
GTU Full Professor

WHAT IS CRYPTOGRAPHY?

Cryptography (From Greek means “secret writing”) is the practice and study of techniques for secure communication in the presence of third parties.

ENCRYPTION ALGORITHMS

- Classified as symmetric and asymmetric classes.
- Symmetric algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

ENCRYPTION ALGORITHMS

- Asymmetric algorithms, is a class of cryptographic algorithms which requires two separate keys, one of which is secret (or private) and one of which is public. Although difference, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature, whereas the private key is used to decrypt ciphertext or to create a digital signature.

ENCRYPTION ALGORITHMS

- As it is widely known for protection of the information generally symmetric block algorithms shall be applied, as the open key systems speed is quite low.

SYMMETRICAL CRYPTOSYSTEM

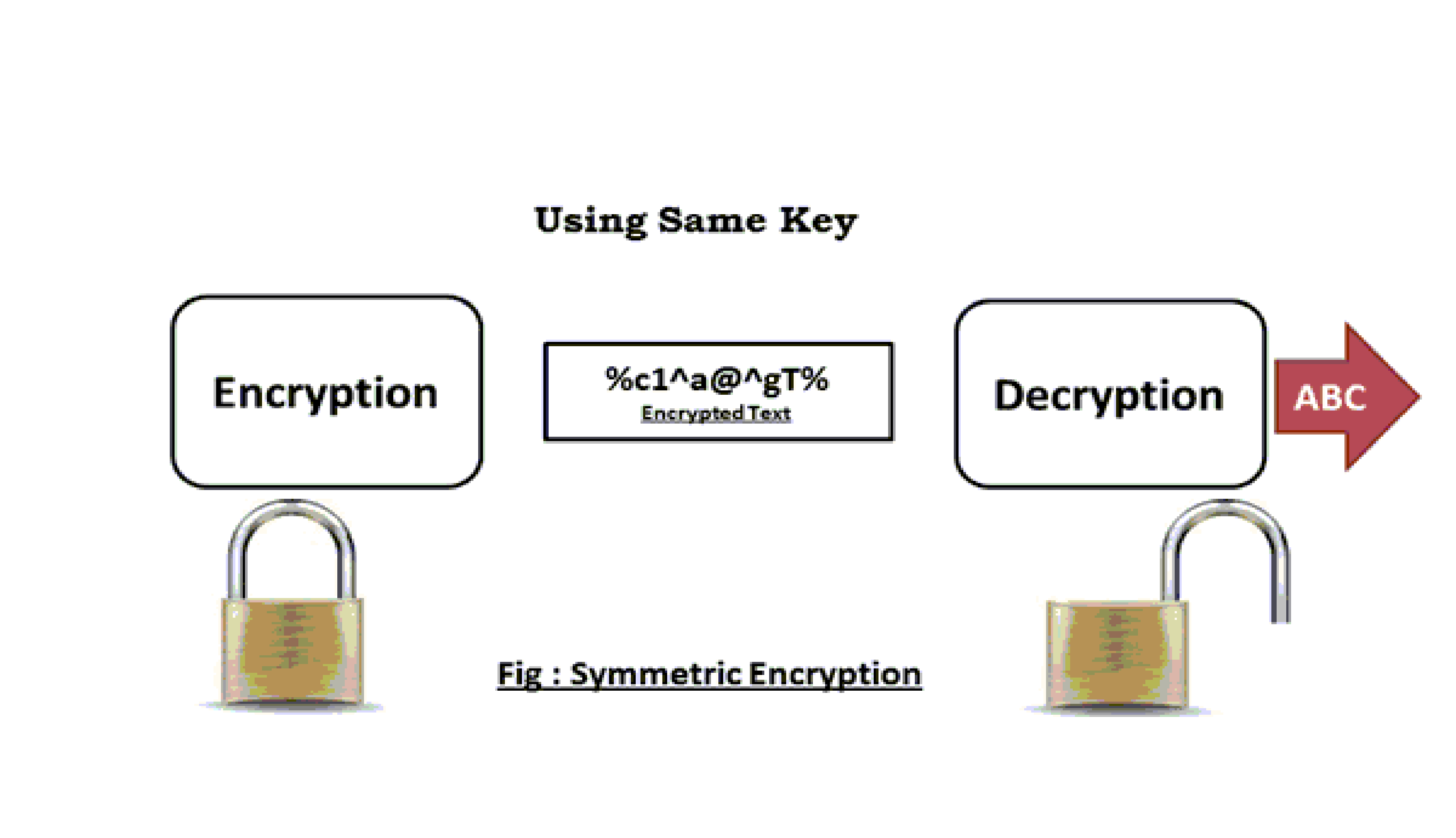


Fig : Symmetric Encryption

SYMMETRICAL CRYPTOSYSTEM

- In order to cover the open text structure the most effective way is to apply for two transformations: ***confusion*** and ***diffusion.***
- ***Confusion*** is the transformation, the goal of which is to cover the connection among the keys and the ciphertext, and the goal of the ***diffusion*** is to render each symbol of the ciphertext dependent onto all the symbols of the open text, which would enable us to cover the open text structure.

SYMMETRICAL CRYPTOSYSTEM

- As in symmetric algorithms it is impossible to use the complex mathematical transformations (that diminishes the fast action of the algorithm), in order to achieve such goals in the modern symmetric cryptography replacement and displacement operations are applied for with the multiple iterations.

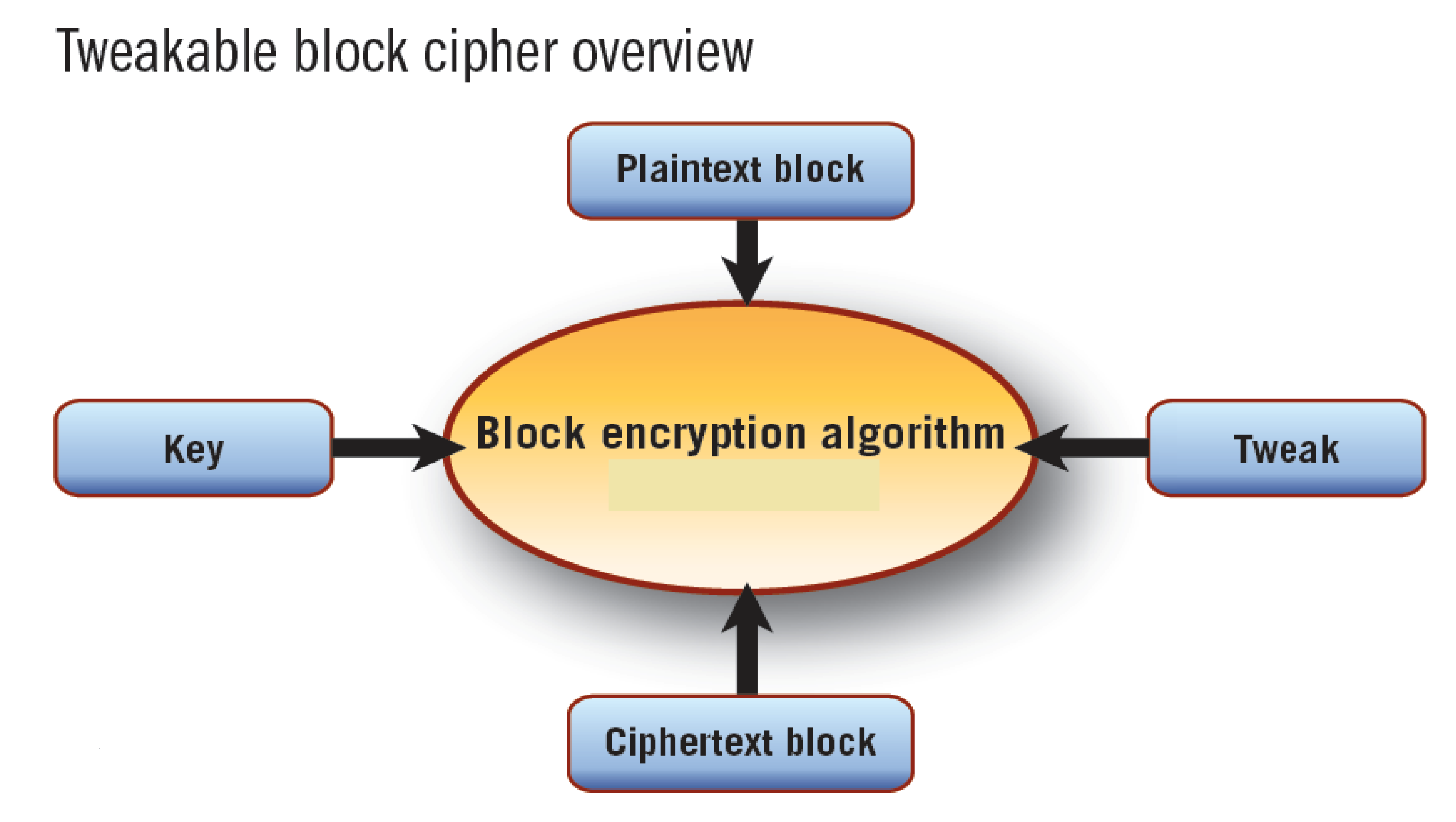
SYMMETRICAL CRYPTOSYSTEM

- Unfortunately, the block ciphers have significant fallback. That is their determined nature, which is expressed in the fact that the same text by means of the same keys is always transferred into the same cipher text. This fallback is tried to be suppressed by means of the encrypting regimes, in which the initialization vector is applied for, which enables to transfer the same text with the same keys into various cipher texts.

TBC

- In 2002 the Article by M. Liskov, R. Rivest and D. Wagner was published, the idea stated in which that, initialization vector might be used not in the regime of encrypting, but in the algorithm itself. Such ciphers are called tweakable block ciphers.

TBC



Tweakable block cipher overview
Plaintext block
Key
Block encryption algorithm
Tweak
Ciphertext block

HILL ALGORITHM

- In 1929 American mathematician Lester S.Hill by means of utilization of the linear algebra created n-gram encrypting algorithm, which enables to make one outgoing symbol of the ciphertext dependet onto the n number of the incoming symbols.

MODIFIED HILL ALGORITHM

- Our goal is to construct tweakable block cipher algorithm, in which in order to cover efficiently the open text structure, by us modified Hill's algorithm shall be used. In crypto algorithm 256 bits block is encrypted with the confidential keys. Upon entrance into the algorithm, the block to be encrypted shall be represented by means of the matrix, which is called the standing matrix, where each is the binary byte. Binary line to be encrypted shall be recorded in the matrix from the left to the right horizontally.

MODIFIED HILL ALGORITHM

$$M=\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

- All the operations, which are completed for the text to be encrypted into the algorithm, are completed on this matrix. We will deal with one operation only, which provides the open text structure effective covering into the ciphertext.

MODIFIED HILL ALGORITHM

- This operation mathematically might be recorded quite simply: $M \times A (\mathrm{mod} 256)$. Where A is the matrix and that matrix shall by all means have the reverse matrix.

```
while(noSuccess)
{
        tryAgain();
        if(Dead)
                break;
}
```

ENCRYPTION

- Let us suppose we have open text: ***Evariste Galois was a French mathematician***. We take the starting 16 symbols, transform them into ASCII code, the obtained result into binary system and adding to the first half of the initial key. Then finding multiplicative inverse for each byte in GF(2^8) field:

E	v	a	r	i	s	t	e
69	118	97	114	105	115	116	101
space	G	a	l	o	i	s	space
32	71	97	108	111	105	115	32

ENCRYPTION

00111101	00011011	11001011	10100100
11110110	11110011	11100000	11011001
11011100	01000110	01000010	10111110
11001011	10100110	01000010	11000100

The obtained binary string we transfer into the decimal system and represent 4x4 dimensional A matrix:

ENCRYPTION

61	27	203	164
246	243	224	217
220	70	66	190
203	166	66	196

N matrix calculated by us in advance:

ENCRYPTION

N Matrix:

-1	-2	-2	-2
2	-1	-2	2
1	1	1	2
-1	1	2	-1

ENCRYPTION

A matrix is multiplied for N matrix, as the result of which 4x4 dimensional A_1 matrix is received again:

32	218	355	174
247	-294	-320	225
-204	-254	-134	-358
-1	-310	-280	-138

The received A_1 matrix is brought with 256 module and transferred into the binary system:

32	218	99	174
247	218	192	225
52	2	122	154
255	202	232	118

ENCRYPTION

32	218	99	174	247	218	192	225
00100000	11011010	1100011	10101110	11110111	11011010	11000000	11100001
52	2	122	154	255	202	232	118
00110100	00000010	1111010	10011010	11111111	11001010	11101000	01110110

ENCRYPTION

- Then binary string is summarized with formed round first key by means of XOR,
- Key 1.1.

00110110	00100011	10001100	01101000	00111001	10010010	11001110	11010010
01100001	11111100	11001101	01111110	01000111	11111110	00010011	11010100

Binary string and Key 1.1. XOR summarization result:

00010110	11111001	11101111	11000110	11001110	01001000	00001110	00110011
01010101	11111110	10110111	11100100	10111000	00110100	11111011	10100010

ENCRYPTION

- The Result is summarized with Tweak entrance by means of XOR:
- Tweak 1.1.:

01001010	10011110	10110001	10011100	00110101	0010101	01001111	01110010
11101111	10110010	01000111	10010010	10110100	01101110	01111001	00011000

In result we get this binary string:

01011100	01100111	01011110	01011010	11111011	01011101	01000001	01000001
10111010	01001100	11110000	01110110	00001100	01011010	10000010	10111010

ENCRYPTION

- Then we transfer it to the decimal system and get next round first data:

92	103	94	90	251	93	65	65
186	76	240	118	12	90	130	186

ENCRYPTION

- With the analogue method we act at B matrix only instead of N matrix we use M matrix and result is:
- M Matrix

-2	-1	2	2
-2	-2	-1	-2
1	1	1	2
2	1	-1	-1

DECRYPTION

w	a	s	space	a	space	F	r
119	97	115	32	97	32	70	114
e	n	c	h	space	m	a	t
101	110	99	104	32	109	97	116

01111000	01100011	11010000	11111011
10001011	00111000	01001011	01011001
10101110	11101101	00010111	01100110
10010111	01011011	10111101	10101011

ENCRYPTION

- And at the end we get next round second data:

200	227	246	129	41	177	31	49
87	34	111	62	109	208	226	110

DECRYPTION

- Decryption is the reversed process of encryption with the insignificant differences. While encrypting instead of the applied N and M matrixes we use 256 module reversed N^{-1} and M^{-1} matrixes accordingly.

N^{-1} matrix:

-1	2	-2	2
-2	-1	-2	-2
1	1	1	2
1	-1	2	-1

DECRYPTION

- M^{-1} matrix:

-2	-1	2	2
-2	-2	-1	-2
1	1	1	2
2	1	-1	-1

CONCLUSIONS

- In our work is done an attempt to build a new tweakable block cipher, which in our opinion, as a result of our work has been achieved. The algorithm is very fast and can easily be realized, both in hardware and software. The algorithm must be checked and analyzed with a variety of tests. At this point, we can only assess in advance it's cryptoresistant against cryptographic attacks. The current algorithm is cryptoresistant against to all currently known cryptanalysis. We are working on algorithm, if possible, patent algorithm and continue research in this direction.

THANK YOU