GEORGIAN TECHNICAL UNIVERSITY

Informatics and Control Systems Faculty

NEW TWEAKABLE BLOCK CIPHER

Student: Levan Julakidze
Informatics and Control Systems Faculty
Doctorate II year

Leader: Zurab Kochladze
TSU Associated Professor

Leader: 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.

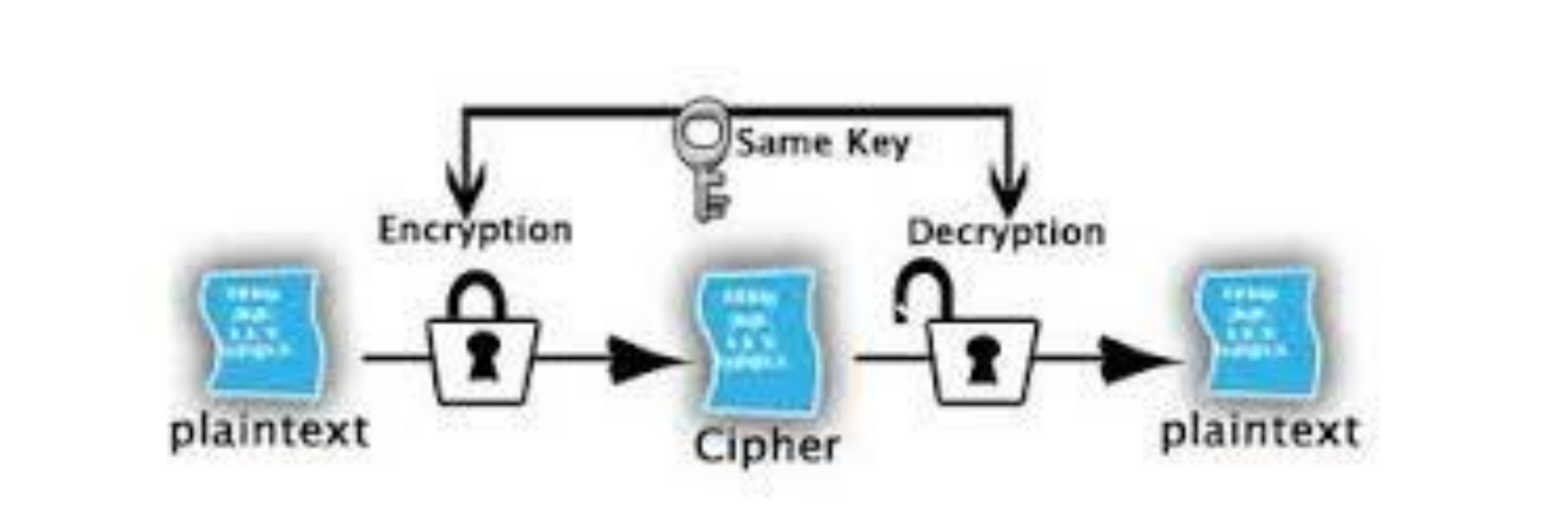
ENCRYPTION ALGORITHMS

- 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



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.

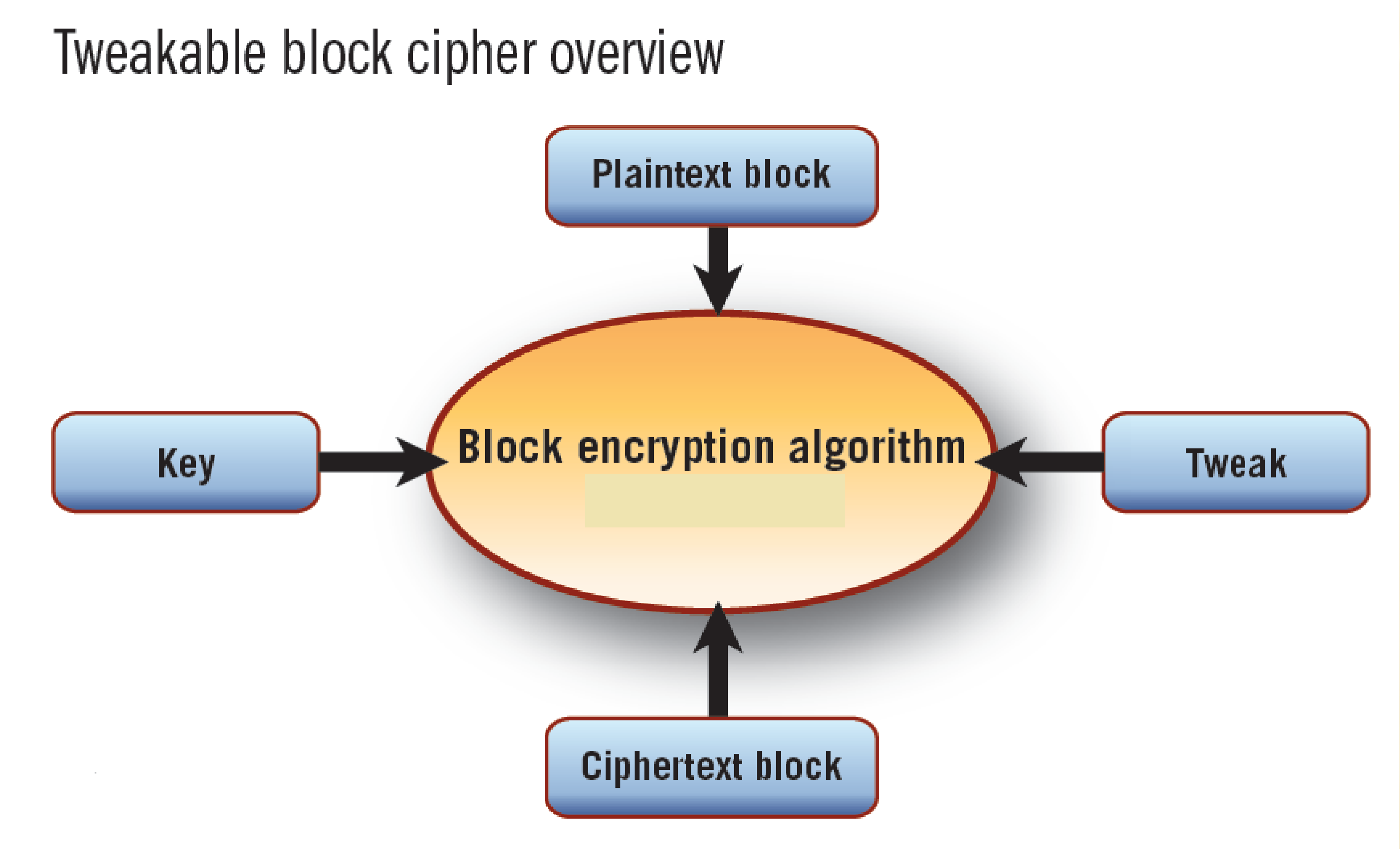
SYMMETRICAL CRYPTOSYSTEM

- 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

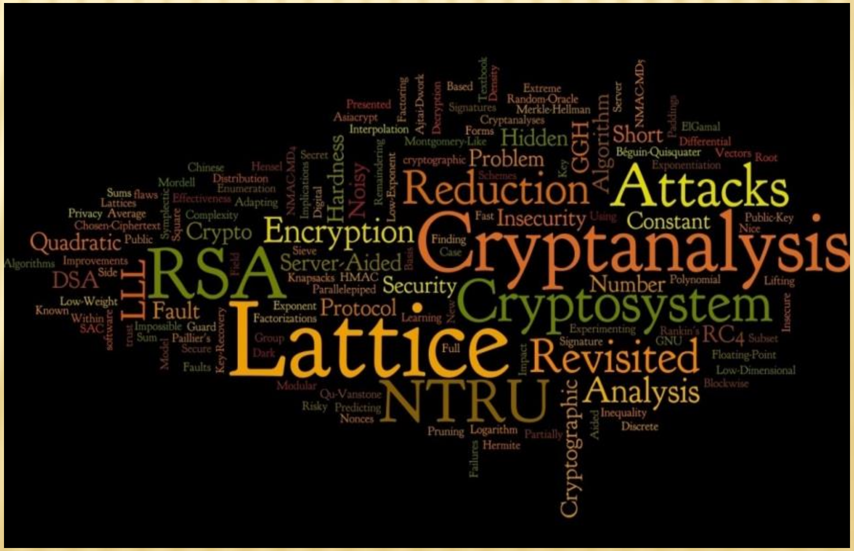
- In 2002 the Article by M. Liskov, R. Rivest and D. Wagner was published, the idea stated in which that, initialization vector might be used not in the regime of encrypting, but in the algorithm itself. Such ciphers are called tweakable block ciphers.

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

- 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.

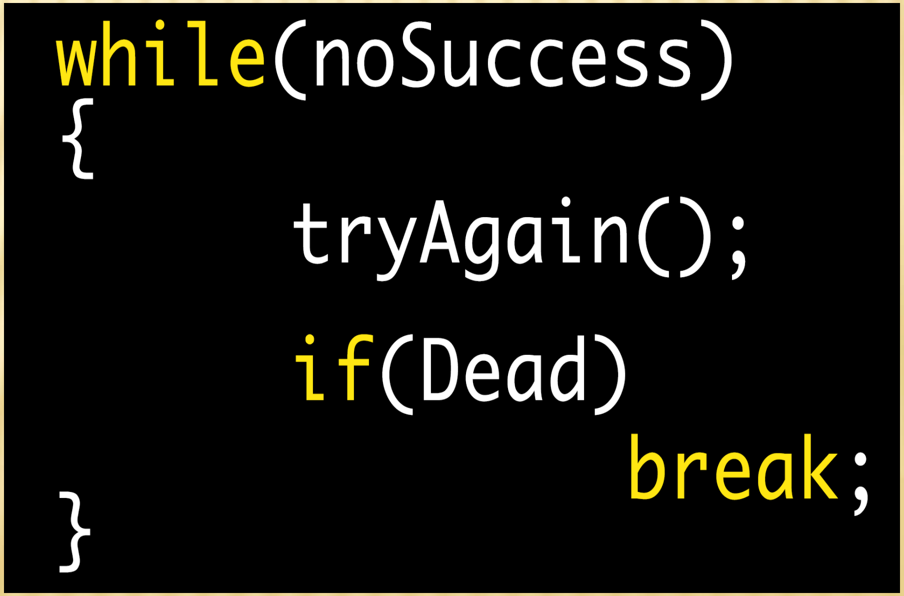
MODIFIED HILL ALGORITHM

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

- 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×A(mod256). 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: If two wrongs don't make a right, try three. We take the starting 16 symbols, transform them into ASCII code and represent 4×4 dimensional A matrix:

I	f	t	w	o	w	r	o
73	102	116	119	111	119	114	111
n	g	s	d	o	n	‘	t
110	103	115	100	111	110	96	116

ENCRYPTION

73	102	116	119
111	119	114	111
110	103	115	100
111	110	96	116

Then we take the following 16 symbol, which we also transfer into ASCII code, represent them as 4×4 dimensional B matrix:

ENCRYPTION

m	a	k	e	a	r	i	g
109	97	107	101	97	114	105	103
h	t	,	t	r	y	t	h
104	116	44	116	114	121	116	104

109	97	107	101
97	114	105	103
104	116	44	116
114	121	116	104

ENCRYPTION

- N and M matrix calculated by us in advance:

N matrix:

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

M matrix:

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

ENCRYPTION

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

128	-13	4	171
130	-116	-124	133
111	-108	-111	116
89	-120	-114	74

ENCRYPTION

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

128	243	4	171	130	140	132	128
10000000	11110011	00000100	10101011	10000010	10001100	10000100	10000000
133	111	148	145	116	89	136	142
10000101	01101111	10010100	10010001	01110100	01011001	10001000	10001110

ENCRYPTION

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

125	165	159	137	90	123	121	73
01111101	10100101	10011111	10001001	01011010	01111011	01111001	01001001
216	200	16	204	121	116	104	114
11011000	11001000	00010000	11001100	01111001	01110100	01101000	01110010

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

- We have considered only a single operation, which provides the open text structure effective covering into the ciphertext. In our case 127 bits changed from 256 bits, which is good result.
- The algorithm is currently under construction and will be available in the near future, the possibility of his performances.

THANK YOU FOR YOUR ATTENTION