electronic periodical
YOUTH SCIENTIFIC AND TECHNICAL BULLETIN
Bauman MSTU Publ EL № FS-77-51038, ISSN 2307-0609

UDK 003.26

COMMUNICATION MODEL IN CRYPTOGRAPHY AND ALGEBRAIC ATTACKS ON STREAM CIPHERS

Khuzina E.I., *student*
«Information Security» department
BMSTU, Moscow, Russia

Scientific supervisor: Matveev V.A., Doctor of Technical Sciences, professor in «Information Security» department of BMSTU
bauman@bmstu.ru

Communication model

Cryptology - the science of secret writing in all its forms, covering both cryptography and cryptanalysis [3]. Cryptanalysis is the science of deducing the plaintext from a ciphertext, without knowledge of the key. Cryptography is the science of encrypting a message, or the science of concealing the meaning of a message. Sometimes the term is used more generally to mean the science of anything connected with ciphers, and is an alternative to the term cryptology [2].

Shannon described the principle of encryption in as a modification of his well-known communication model. It involves two entities, usually referred to as sender and receiver. The sender's goal is to confidentially transmit some data, named the plaintext, to the receiver. For this purpose he has access to two different communication channels:

1. Secret channel. The secret channel is completely confidential. None of the data transmitted over this channel can be eavesdropped by anybody except sender and receiver. However, the usage of this channel is limited to certain time points, e.g. when sender and receiver are in the same place.
2. Public channel. The public channel can be used anytime to transmit data of arbitrary size. Yet, it is insecure in so far as anybody can listen to the transmitted messages.

It is necessary to introduce a third party, called the attacker. An attacker's goal is to derive some secret information, for instance the plaintext P and/or the secret key K. The algorithm deployed by him will be called attack [1].

Definition 1. A cryptosystem or cipher is a five-tuple $(P, C, \mathcal{K}, E, D)$, such that the following conditions are satisfied [1]:

•P is a finite set of possible plaintexts.

•C is a finite set of possible ciphertexts.

•$\mathcal{K}$, the keyspace, is a finite set of possible keys.

•$E : \mathcal{K} \times P \rightarrow C$ is the encryption algorithm

•$D : \mathcal{K} \times C \rightarrow P$ is the decryption algorithm

•For each $K \in \mathcal{K}$, it holds that $D(K, E(K, P)) = P$ for all $P \in P$.

Cryptosystems can be symmetric (AES, DES) or asymmetric (DSS, RSA). In a symmetric system the sender and receiver establish secret key that is used for encryption and decryption. In an asymmetric cryptosystem the sender encrypts with the receiver's public key and the receiver can then decrypt using his private key.

There are two types of symmetric cryptosystems: stream ciphers and block ciphers. Stream ciphers encrypt individual characters of a plaintext per one time unit, using an encryption transformation usually is different in different time period. By contrast, block ciphers encrypt groups of plaintext symbols using a constant encryption transformation.

One of the construction the stream ciphers methods is derived from the one-time pad. Let $P = C = \mathcal{K} = \{0, 1\}$ for some integer $n \geq 1$. The encryption algorithm is defined as $E_K(P) := K \oplus P$ where $\oplus$ denotes the componentwise XOR. The corresponding decryption function is $D_K(C) = K \oplus C$. Keystream generators are used to produce a key K.

The one-time pad is infeasible for practical applications, as it would require to manage keys of the same size as the data that has to be encrypted. Thus, instead of using random keys of the same size as the message, one uses smaller keys to initialize a keystream generator to generate pseudo-random bitstreams of the length of the plaintext, giving a pseudo one-time pad.

It has been proved that one-time pad cryptosystem is perfectly secure if K is used only once (therefore the name one-time pad) and is chosen uniformly distributed from {0, 1}. Thereby, perfectly secure means that if an attacker knows only C, then it is impossible for him to gain any information about P and/or K, even with unlimited time, memory and computational resources.

Sender and receiver encrypt their messages as follows [1]:

1. Sender and receiver agree on a secret key $K \in \mathcal{K}$. Therefore, the secret channel is used to exchange all necessary data. This has to be done only once.

2. Let $P = (p_0, p_1, p_2, \ldots)$ with $p_t \in P$ denote the plaintext. The sender uses K and the keystream generator to generate a keystream $z_0, z_1, z_2, \ldots$ and encrypts P to $C := (c_0, c_1, c_2, \ldots)$ with $C_t := Ez_t(p_t)$. C is send to the receiver over the public channel.

3. The receiver, who has knowledge of the secret key K, can generate the same keystream $z_0, z_1, z_2, \ldots$ on his own.

4. Knowing the keystream, the receiver decrypts pt = Dzt(ct).

Algebraic attacks

In cryptography, the stream cipher is claimed to be secure if and only if the underlying keystream generator is secure. For the security analysis of a keystream generator, we consider the following attack model. An attacker knows all public information as for example the exact specifications of the keystream generator. Additionally, he is able to observe the values of some of the keystream elements. The attacker's goal is to find out the secret key K. If he is successful, he can compute the keystream for himself and easily decrypt the whole ciphertext.

To evaluate the efficiency of an attack, we will consider the following three values [1]:

1. The number of data needed, e.g. the amount of plaintext and/or ciphertext.
2. The run time to perform the attacker, that is the number of basic operations.
3. The amount of memory required to store information for an attack

Algebraic attacks - a method of cryptanalytic attack used against block ciphers and stream ciphers that exhibit a significant amount of mathematical structure. Any stream cipher is defined by a system of algebraic equations. A solution of this system gives the secret key. Algebraic attacks on LFSR-based stream ciphers recover the secret key by solving an over defined system of multivariate algebraic equations [1].

The problem of finding a solution to a random system of quadratic equations is NP-complete. On the other hand, the case of linear systems of equations is rather easy as they can be solved efficiently by Gaussian elimination. Here, efficiently means that time and memory effort are polynomial in the number of unknowns. For the case of non-linear equations, one also has to deal with products of unknowns. The key idea of linearization is to re-write the system of nonlinear equations in n unknowns as a new system of linear equations with a significantly increased number of unknowns, which can be easily solved by Gaussian elimination. We reduced the problem of solving the system of non-linear equations to computing the kernel space of the matrix of system of equations coefficients.

One of the algebraic attacks types is fast algebraic attacks. The system of equations is used to reveal the stream cipher key. The properties of the equations allow for reducing the

overall degree of the system of equations in an efficient pre-computation step. This method is an enormous speed-up of the whole attack. In this method each equation is divided into two parts: the first part is of high degree, the second – low degree. The main idea of reducing the system overall degree is to eliminate high degree parts of the equations by calculating a linear combination of several equations, and to get a new functions of lower degree. There is a theorem about an existence of such coefficients in linear combination that the sum of high degree parts of some equations is zero. If the degree reduction is achievable with sufficiently little effort, fast algebraic attacks are superior to algebraic attacks.

Conclusion

Using asymmetric or symmetric cryptosystems depends on the whole systems data is transmitted in. One of the symmetric cryptosystems is stream ciphers, they are effective in transactions, where high speed and continuity are required. These ciphers encode one character per one time unit. In contrast, block ciphers encode block of bits and transmit block per one time unit. There are algebraic attacks on stream ciphers. They use system of equations, the system consists of equations for each element of set keystream known elements. The linearization method and fast algebraic attack are applied to speed up the whole attack on stream cipher.

References

1. Armknecht F. Algebraic attacks on certain stream ciphers: Inauguraldissertation zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften / Universitat Mannheim. Mannheim. 2006. 217 p.
2. Mollin R. A. An Introduction to Cryptography. CRC Press, 2007, 413 p. ISBN 1584886188.
3. Simon Singh. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Books, 2000. ISBN 0385495323.