DOI: 10.18372/2225-5036.30.18614

RATIONALE FOR IMPROVING AUTHENTICATION PROTOCOLS IN THE CONDITIONS OF POST-QUANTUM CRYPTOGRAPHY

Alla Havrylova[1], Iryna Aksonova[2], Yuliia Khokhlachova[3], Tetiana Milevska[4], Sergii Dunaiev[5]

[1, 2, 4, 5]National Technical University "Kharkiv Polytechnic Institute", Ukraine

[3]National Aviation University, Ukraine

Alla HAVRYLOVA, PhD, associate professor
Date and place of birth: 1972, Molodogvardeysk, Krasnodon district, Luhansk region.
Education: Kharkiv National University of Radio Electronics, 2021.
Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: cryptographic methods of information security in telecommunication systems.
Publications: more than 30 scientific publications, including monographs, textbooks, articles and patents.
E-mail: alla.havrylova@khpi.edu.ua.
Orcid ID: 0000-0002-2015-8927.

Iryna AKSONOVA, candidate of economic sciences, associate professor of cybersecurity department
Date and place of birth: 1973, R. Lozovaya, Dergachevsky district, Kharkiv region.
Education: Kharkiv National University of Economics, 1995.
Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: quantitative methods for assessing and analyzing information.
Publications: more than 120 scientific publications, including monographs, textbooks, articles and copyrights.
E-mail: ivaksyonova@gmail.com.
Orcid ID: 0000-0003-2605-0455.

Yuliia KHOKHLACHOVA, candidate of technical sciences, professor
Date and place of birth: 1981, Kyiv, Ukraine.
Education: National Aviation University, 2004.
Position: professor of the Department of information technology security, National Aviation University, Ukraine.
Scientific interests: information security, vulnerability assessment, information systems optimization.
Publications: more than 100 scientific publications, including scientific articles, monographs, textbooks and teaching aids.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Tetiana MILEVSKA, senior lecturer
Date and place of birth: 1980, Kharkiv, Ukraine.
Education: Kharkiv National University of Economics, 2002.
Position: senior lecturer of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: information security, social security.
Publications: more than 20 scientific publications, including monographs, textbooks, articles and patents.
E-mail: milevskats@gmail.com.
Orcid ID: 0009-0006-5218-9353.

Sergii DUNAIEV, PhD student
Date and place of birth: 1991, Kharkiv, Ukraine.
Education: Kharkiv Polytechnic Institute, 2023.
Position: PhD student of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: information protection in socio-cyberphysical systems.
Publications: 4 articles publications.
E-mail: serg.dynaev@gmail.com.
Orcid ID: 0000-0001-8736-3602.

Abstract. *The paper studies the relevance of the issues of encrypting confidential data for their transmission over unsecured channels of information and communication networks. An analysis of encrypted information exchange on the Internet based on the Google service was carried out in terms of the volume of encrypted web traffic. It is concluded that the difference in traffic volumes between countries is due to the popularity of the types of devices used, the geographic access infrastructure, as well as the availability of software that provides modern types of encryptions. The role of the HTTPS protocol in ensuring the security of working with resources on the Internet is substantiated. The NIST security requirements for modern information and communication systems in the post-quantum period are analyzed. It is determined that within a short period of time the power of computing devices increases exponentially, which entails an increase in the implementation of both already known and new attacks on cryptographic algorithms that ensure the strength of security services in networks. Based on the results of this study, the results of a comparative analysis of the complexity of classical and quantum algorithms were demonstrated. The classification of special attacks was considered according to the signs of influence on computing processes, according to access to systems and means, as well as according to the specifics of the attacks themselves. Solutions submitted for participation in the NIST competition for the definition of security standards through electronic digital signature mechanisms, encryption algorithms and key encapsulation are analyzed. The results of the analysis are presented in the form of a scheme of security and stability of the proposed protocols and algorithms. It is recommended to use TLS protocols to ensure the integrity and authenticity of users when establishing communication sessions with websites. A scheme of the process of authenticated encryption and authentication of an encrypted message transmitted over a TLS connection has been developed. A process scheme has been developed for authentication encryption and decryption of information when establishing a communication session in TLS protocols. A comparative analysis of the characteristics of the TLS 1.3 and TLS 1.2 protocols was carried out.*

Keywords: *NIST, HTTPS, TLS, digital signature, combined encryption algorithms.*

Introduction

In connection with the ever-increasing volumes of information transfer containing confidential data through insecure Internet channels, the need to protect this data during transmission and storage in cloud services increases in direct proportion. Consequently, there is a growing need to change approaches to their encryption in the case of using quantum computers to obtain unauthorized access by cryptanalysts.

Analysis of existing studies

Thus, according to the “Report on the availability of services and data” [1, 21], the amount of encrypted information exchange on the Internet today in the Google service depends on the specific country. (fig. 1).

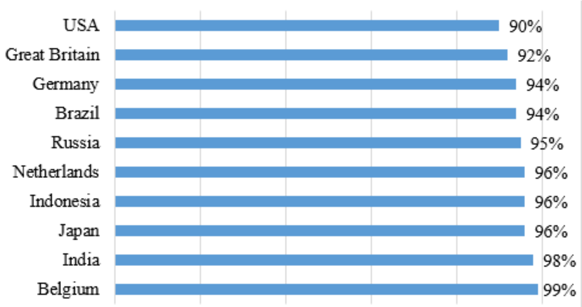

Fig. 1. Volume of encrypted web traffic as of 01/01/2023

This graph shows the volume of encrypted web traffic in the top ten countries that passes through the Google service. The difference in traffic between countries is due to a number of factors, including the popular types of devices used in certain countries and the availability of software that supports modern encryption technologies such as TLS protocols. Computer users load more than half of the pages over HTTPS and spend two-thirds of their time on them. Thus, the percentage of pages loaded via HTTPS in Chrome has more than doubled since 2018 and, as of 04.02.2023. amounted to 99%, the dynamics of switching to HTTPS for different platforms and countries has the same upward trend. On mobile devices, HTTPS is not yet widely used, but here it is growing.

Purpose and statement of the task

Therefore, the purpose of this work is to study the use and justification of directions for improving authentication protocols in the context of post-quantum cryptography.

The main part of the study

Analysis of security requirements in modern information and communication systems and networks

The development of computing resources in recent decades confirms their growth in accordance with the assumptions made by Gordon Moore (founder of Fairchild Semiconductor and also Intel) according to his empirical observations. In accordance with his conclusions, every 18 months the performance of computing technology increases by 2 times, that is, every 5–10 years, performance increases by 3–5 orders of magnitude (1000–100000 times). If this trend continues, then the power of computing devices will increase exponentially over a relatively short period of time. Thus, intruders and cybercriminals have computing power that allows them to implement attacks on cryptographic algorithms that ensure the durability of security services. In addition, in 1994, an algorithm developed by the American mathematician Peter Shor appeared. It made it possible to factor an integer of arbitrary length into prime factors almost as quickly as to multiply them. Shor's algorithm allows you to factorize the number N in O(lg3N) time using O(lg N)-bit register, which is much faster than any classical factorization method. The advantage of using quantum registers is significant memory savings (N quantum bits can contain 2N bits of information), and the interaction between qubits makes it possible to affect the entire register in one operation (quantum parallelism).

Thus, Shor's algorithm called into question the very existence of asymmetric cryptography, since on its basis it is possible to effectively solve problems of discrete logarithm and other problems on the complexity of which cryptographic algorithms are based. This conclusion was confirmed in March 2018 in a report by NIST (National Institute of Standards and Technology), USA (Report on Post-Quantum Cryptography) [2, 3, 4, 5, 6, 7], which notes that the emergence of full-scale of quantum computers calls into question the cryptographic strength of asymmetric cryptography algorithms, and in February 2019, NIST specialists, at the opening of a competition for post-quantum cryptography algorithms, announced that algorithms on elliptic curves are also being questioned. Thus, humanity is entering the post-quantum period - a period of time in the future, when classical methods will be significantly improved and quantum computers will be created with the register lengths (in qubits) necessary for successful cryptanalysis and the mathematical and software necessary for their implementation. The main tasks that can be solved on a quantum computer include the following [2, 8, 16, 19]:

1) quantum Shor factorization algorithm;

2) Grover's quantum algorithm for finding an element in an unsorted base;

3) Shor's quantum algorithm for solving a discrete logarithm in a finite field;

4) a quantum algorithm for solving a discrete logarithm in a group of points of an elliptic Shor curve;

5) quantum cryptanalysis algorithms for transformations into ring factors;

6) the quantum algorithm of cryptanalysis by Xiong and Wang and its improvement.

Table 1 shows the results of a comparative analysis of the complexity of factorization for classical and quantum algorithms [13, 19], Table 2 shows the complexity of implementing the Shor method of discrete logarithm in a group of points of an elliptic curve [13, 19, 22-25].

Table 1

Comparative analysis of factorization complexity for classical and quantum algorithms

Module size N, bit	Number of qubits needed $2n$	The complexity of the quantum algorithm $4n^3$	The complexity of the classical algorithm
512	1024	0.54 ·109	1.6 ·1019
3072	6144	12 ·1010	5 ·1041
15360	30720	1.5 ·1013	9.2 ·1080

Table 2

The complexity of implementing the Shor method of discrete logarithm to a group of points of an elliptic curve

Algorithm for calculating a discrete logarithmic equation			
Base point order size, bits	Number of qubits needed $f(n) = 7n + 4\ log_2\ n + 10$	The complexity of the quantum algorithm $360n^3$	The complexity of the classical algorithm
163	1210	$1.6 \cdot 10^{9}$	$3.4 \cdot 10^{24}$
256	1834	$6 \cdot 10^{9}$	$3.4 \cdot 10^{38}$
571	4016	$6.7 \cdot 10^{10}$	$8.8 \cdot 10^{85}$
1024	7218	$3.8 \cdot 10^{11}$	$1.3 \cdot 10^{154}$

The results of comparisons presented in Table 1, Table 2 indicate a significant reduction in energy costs for the implementation of breaking cryptographic algorithms of asymmetric cryptography, which include electronic digital signature algorithms.

In the context of post-quantum cryptography, NIST experts suggest considering a special type of attack (SIDE-CHANEL ATTACKS). The implementation of these attacks is aimed at finding vulnerabilities in the practical implementation of the cryptosystem, primarily the means of cryptographic protection.

The following classification of special attacks is proposed according to the following criteria [14]:

– control over the computing process;

– method of access to the system or means;

- a method of direct attack, and the like.

Features [15] can be used as the basis for protection against attacks of a special type:

– a fixed number of hash function calls, data randomization;

– independence of keys from values and the like.

As part of cybersecurity monitoring, the NIST Computer Security Center (CSRC) has created three working groups, in which all the activities of the center are divided into major areas [16]:

• information security management;

• technical issues of information security;

• cryptographic protection of information.

Each group has generated dozens of publications to date. Many documents are reviewed regularly. For many years, NIST documents (special publications and standards) have been used by the global cybersecurity community to build coherent, transparent, measurable information security and cyber risk management processes. As part of the cryptographic protection of information, a search is made for cryptoalgorithms that are resistant to selection on a quantum computer. The chosen encryption algorithms will become part of the NIST post-quantum cryptographic standard. The solutions submitted for participation by NIST implement the following mechanisms [9]: digital signature, encryption, key encapsulation, and pre-shared key generation. NIST sets requirements for resistance to contestants, both formal (strictly provable based on the assumption of the complexity of solving a particular problem) and practical. Among strictly evidentiary requirements, based on the assumption of the complexity of solving a certain problem, there are requirements for asymmetric encryption and electronic digital signature systems [2, 17]. Asymmetric encryption systems are characterized by such requirements as:

- Indistinguishability Against Chosen Plaintext Attack (IND-CPA) ciphertext recognition threat;
- resistance to the threat of ciphertext recognition based on an attack based on a chosen ciphertext (Indistinguishability Against Chosen Ciphertext Attack, IND-CCA);
- Indistinguishability Against (non-adaptive) Chosen Plaintext Attack, IND-CPA1;
- Indistinguishability Against (non-adaptive) Chosen Ciphertext Attack, IND-CCA1;
- resistance to the threat of ciphertext recognition based on an attack based on an adaptively chosen plaintext (Indistinguishability Against Adaptive Chosen Plaintext Attack, IND-CPA2);
- resistance to the threat of recognition of ciphertexts based on an attack based on an adaptively chosen ciphertext (Indistinguishability Against Adaptive Chosen Ciphertext Attack, IND-CCA2).

For electronic digital signature schemes, the following concepts of stability are of interest:

- strong resistance to forgery attacks based on selected messages (Strong Unforgeability under Chosen Message Attacks, SUF-CMA);
- Existentially Unforgeability under Chosen Message Attacks (EUF-CMA) attacks.

The NIST definitions of practical durability suggest five levels of durability [11]:

1) determining the key of a 128-bit block cipher;
2) search for a collision of a 256-bit hash function;
3) determining the key of a 256-bit block cipher;
4) search for a collision of a 384-bit hash function;
5) determination of the key of the 384-bit block cipher.

The main solutions used by NIST contestants fall into six groups [3, 9]:

- the use of the theory of integer lattices - based on a number of complex problems, including NP-problems of finding the shortest vector (SVP) and finding the nearest vector (CVP);
- problem of learning with errors (LWE; RLWE) and the problem of finding the smallest integer solution to the system of linear algebraic equations (SIS);
- the use of error-correcting codes - the McEliece scheme remains stable when using Goppa codes;
- the use of polynomials in many variables - is studied from the point of view of the synthesis of crypto schemes;
- the use of cryptographic hash functions - one-time signatures of Lamport and Winternitz are used, adapting them to build a multiple signature scheme based on a tree structure of hash values of a special type;
- the use of isogenies on supersingular elliptic curves - the solution of the complex problem of finding a path in the graph of isogenies between supersingular elliptic curves is the basis;
- highly specialized problems (Search Problem or operations in Braid Groups), octonion algebra, Chebyshev polynomials, etc.

The main NIST requirements for safety and stability in the conditions of the post-quantum period [18] are presented (fig. 2).

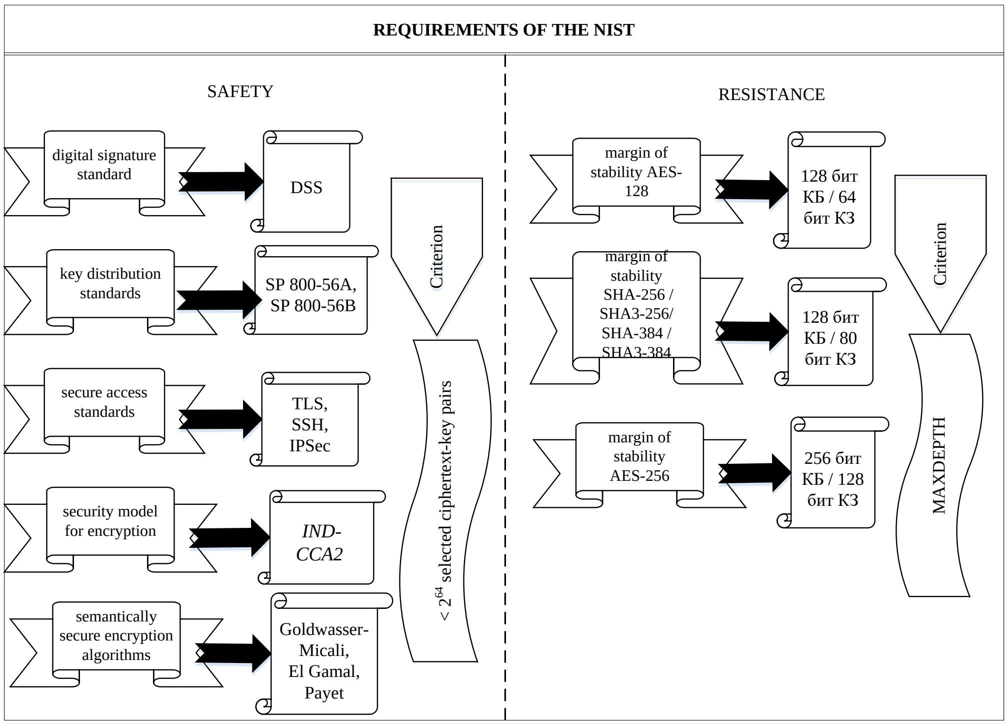
REQUIREMENTS OF THE NIST
SAFETY
RESISTANCE
digital signature standard
DSS
key distribution standards
SP 800-56A, SP 800-56B
secure access standards
TLS, SSH, IPSec
security model for encryption
IND-CCA2
semantically secure encryption algorithms
Goldwasser-Micali, El Gamal, Payet
Criterion
< 2^64 selected ciphertext-key pairs
margin of stability AES-128
128 бит КБ / 64 бит КЗ
margin of stability SHA-256 / SHA3-256/ SHA-384 / SHA3-384
128 бит КБ / 80 бит КЗ
margin of stability AES-256
256 бит КБ / 128 бит КЗ
Criterion
MAXDEPTH

Fig. 2. NIST Requirements for Security and Persistence in Post-Quantum Conditions

According to the information presented in the diagram, there are two groups of requirements, through the observance of which, it is possible to increase the degree of resistance to the actions of a cryptanalyst when he uses a quantum computer.

So, within the framework of safety requirements, it is recommended [5, 20].

I. As an electronic signature standard, use DSS (Digital Signature Standard) [6], which was adopted in America and is based on the FIPS-186 document and the DSA (Digital Signature Algorithm) algorithm. DSA (Digital Signature Algorithm) refers to algorithms using a public key to create an electronic signature.

The signature is created secretly but can be publicly verified. This means that only one subject can create a message signature, but anyone can verify that it is correct. The algorithm is based on the computational complexity of taking logarithms in finite fields. The algorithm was proposed by NIST in August 1991 and is patented by U.S. Patent 5,231,668, but NIST has made this patent available for royalty-free use. The algorithm, together with the SHA-1 cryptographic hash function, is part of the DSS (Digital Signature Standard), first published in 1994 (document FIPS-186 (Federal Information Processing Standards)). Later, 2 updated versions of the standard were published: FIPS 186-2 (January 27, 2000) and FIPS 186-3 (June 2009).

II. Use SP 800-56A and SP 800-56B (Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography) [7] as key distribution standards:

1) SP 800-56A defines key derivation schemes based on the discrete log problem over finite fields and elliptic curves, including several variations of Diffie-Hellman and Menezes-Couvanston (MQV) key derivation schemes;

2) SP 800-56B defines key derivation schemes using integer factorization cryptography based on ANS X9.44, key derivation using integer factorization cryptography [ANS X9.44], which was developed by Accredited Standards Committee (ASC) X9, Inc.

III. Using the new standard in protocols: TLS, SSH, IPSec [6]:

1) TLS (Protocol for Secure Data Transfer over an Insecure Network with Privacy, Integrity, and Authentication) is the new TLS 1.3 standard.

2) SSH using keys. SSH is a protocol for secure access to remote systems. SSH is mainly used to access servers, to remotely access the console, to the terminal, to the shell of a remote machine (mainly a Linux operating system, but there may be other network equipment or even a device with a Windows operating system). The use of keys has a number of security-related advantages: they are difficult to break (a sufficient key length provides robust cryptographic resistance to brute-force or dictionary attacks); when using keys on the server, no private information is stored;

3) IPSec is a protocol for protecting network traffic, which, despite its excessive complexity and redundancy, has a number of important properties that allow it to provide the required level of security: hardware independence; no code changes required for applications; The IP packet provides protection in its entirety, including protection for higher layer protocols; packet filtering based on authenticated headers, source and destination addresses, which provides simplicity and low cost, suitable for routers; transparent to users and applications.

IV. Security model for IND-CCA2 encryption [2].

V. Distributed "semantically secure encryption" scheme [3].

This scheme is intended to allow for the use of encryption algorithms that support a cryptographic system in which only minor information about the plaintext can be extracted from the ciphertext. Semantically secure encryption algorithms are Goldwasser-Micali, El Gamal and Payet. These schemes are considered to be provably secure since their semantic security can be reduced to solving some complex mathematical problem (eg Diffie-Hellman Solver or Quadratic Residuality Problem). In this case, the security criterion is an attacker's access to less than 264 selected ciphertext-key pairs.

With regard to durability requirements, the following is recommended [4].

I. 128 bits of classical security / 64 bits of quantum security, which ensures the safety margin of AES-128.

II. 128 bits of classical security / 80 bits of quantum security, which ensures the safety margin of SHA-256 / SHA3-256 / SHA-384 / SHA3-384.

III. 256 bits of classical security / 128 bits of quantum security, which provides a headroom for AES-256.

In this case, the resistance criterion is the MAXDEPTH parameter, in which quantum attacks are limited by a set of fixed operating time, or "depth" of the scheme:

– 2^{40} logic gates, that is, the approximate number of gates that will be sequentially executed per year;

– 2^{64} logic gates, which modern classical computing architectures can perform sequentially in ten years;

- no more than 2^{96} logic gates, that is, an approximate number of gates, as atomic scale qubits with the speed of light of propagation time can perform in millennia.

Thus, NIST suggests considering the following models:

– for symmetric cryptography algorithms – under the conditions of the IND-CCA2 (Indistinguishability Adaptive Ciphertext Attack) security model, which determines resistance to an adaptive attack based on the selected ciphertext;

– for an electronic digital signature – under the conditions of the EUF-CMA security model (existentially unforgeable under adaptive chosen message attacks);

– for the key encapsulation protocol – under the conditions of the Canetti-Krawczyk security model (CK-security).

Regarding the universal algorithms that can be used to protect the transmission of information in information and communication networks, CRYSTALS-Kyber was chosen in the third round, the strengths of which are a relatively small key size and high speed. In addition to CRYSTALS-Kyber, four more general-purpose algorithms were identified - BIKE, Classic McEliece, HQC and SIKE, which, subject to the elimination of identified shortcomings, can be included in the finalists.

The universal algorithms left for refinement are based on other principles: BIKE and HQC used elements of algebraic coding theory and linear codes, also used in error correction schemes. NIST also intends to further standardize one of these algorithms for a lattice theory-based alternative to CRYSTALS-Kyber. The SIKE algorithm is based on the use of supersingular isogeny (circling in a supersingular isogenic graph) and is also considered as a candidate for standardization, since it has the smallest key size. But, as of August 3, 2022, the SIKE post-quantum encryption algorithm was cracked using a regular computer in just one hour [8]. Of the algorithms aimed at working with digital signatures, CRYSTALS-Dilithium, FALCON and SPHINCS+ were singled out. The CRYSTALS-Dilithium and FALCON algorithms are highly efficient. CRYSTALS-Dilithium was recommended as the primary algorithm for electronic digital signatures, FALCON is focused on solutions that require a minimum signature size. SPHINCS+ lags behind the first two algorithms in terms of signature size and speed, but was left as a fallback among the finalists. The CRYSTALS-Kyber, CRYSTALS-Dilithium and FALCON algorithms used cryptography methods based on solving problems of lattice theory, the solution time of which does not differ on conventional and quantum computers. The SPHINCS+ algorithm uses hash-based cryptography techniques. Thus, the analysis showed that the use of an electronic digital signature based on asymmetric cryptoalgorithms in the post-quantum period cannot provide a guaranteed level of cryptographic strength, and, accordingly, can be subject to a special type of attack based on a full-scale quantum computer.

Analysis of modern data transfer protocols in information and communication networks

The main direction of work on the Internet is the transfer of confidential data between the Server and Clients. Such data includes the name and password (authentication data) for entering the control panel, accounts of individuals. And for billing systems, there is much more confidential data - from personal information to financial data. Therefore, ensuring reliable protection of this data is one of the most important tasks.

So, to ensure the integrity and authenticity of users when establishing communication sessions with websites, integrity protocols such as SSL (Secure Socket Layer) or TLS (Transport Layer Security) are used for secure data transfer over an insecure network. Their presence also ensures the integrity of e-mail information flows [5, 6, 9, 20, 21]. For this, various cryptography technologies are used, including encryption, digital signature, certificates, hash functions, MAC. So, earlier encryption was rarely used - mainly on pages where it was necessary to enter password data or credit card data. But, starting in 2018, encryption is starting to be used more often. This is also due to the ubiquity of Internet access from mobile devices, despite the fact that mobile devices have much less computing power than desktop computers and servers. SSL or TLS protocols ensure the integrity of information flows using symmetric encryption algorithms (3DES, AES), and also use MAC codes to provide authentication services.

But SSL protocols and some versions of TLS protocols (TLS 1.1, TLS 1.0) are outdated, as they have security problems, and are not recommended for use, since the technical solutions for combining encryption, authentication, and others that exist on them are not correctly defined. The main place to use TLS is the Internet. All websites that are visited using HTTPS are protected by TLS. Thus, the HTTP protocol is overlaid on top of TLS. By analogy, email with SMTPS is actually SMTP over TLS, and FTPS (Protocol for Secure File Transfer) is also FTP plus TLS.

The importance of using TLS is as follows [10]:

1) authentication implementation: TLS authenticates the communicating parties, which are typically clients and servers; using asymmetric cryptography, a transition to a real website is guaranteed, and not a fake one;

2) providing authentication: TLS protects transmitted data from unauthorized access by encrypting them using symmetric encryption algorithms;

3) integrity implementation: TLS recognizes any changes to the data during transmission by checking the message's authentication code.

The TLS architecture consists of 2 protocols [11].

I - handshake protocol (purpose - authentication and key exchange), on which the Client and the Server perform the following procedures:

- agree on the version of the protocol;
- select a cryptographic algorithm or cipher suite;
- authenticate each other using asymmetric cryptography;
- define the shared secret that will be used for symmetric encryption at the next level.

II - recording protocol. At this level, the following procedures are performed:

- all outgoing messages are encrypted using the secret key set during the handshake;
- encrypted messages are transmitted from the Client to the Server;
- The server checks received encrypted messages for changes;
- if there are no changes, the encrypted messages are decrypted using the secret key.

To ensure that the encrypted message has not been modified during transmission, TLS protocols use authenticated encryption (fig. 3). From the above diagram, it can be seen that the authenticated encryption of a user's message consists of three processes.

The first process is encryption. The sender's text message (M) goes through a symmetric encryption algorithm (AES-256-GCM or CHACHA20). This encryption algorithm also takes as input a shared secret key (K) and a randomly chosen nonce (nonce) or initialization vector (IV). It will return an encrypted message.

The second process is authentication. The unencrypted message (M), secret key (K), and nonce/IV become input to the MAC algorithm, (GCM for AES-256, or POLY1305 for CHACHA20). This MAC algorithm behaves like a cryptographic hash function and produces a MAC (Message Authentication Code) as the output.

Moreover, according to the AES-256-GCM algorithm, the security level of the hash function corresponds to the security level of the keys; however, unlike other modes, SHA-384 is used. More "heavyweight" keys make this cipher somewhat slower, but it is keys of this size that have the advantage of being secure, even if a sufficiently powerful quantum computer is used.

ChaCha20-POLY1305, on the other hand, is an algorithm that takes 512 bits as input and outputs 512 bits in a way that makes it extremely difficult to determine what the input was, and which ensures that each of the output bits is affected by each bit applied to the input. The technique is to create a block with a 256-bit key, a 128-bit constant, and a 128-bit mix of counter value with a value that is used only once.

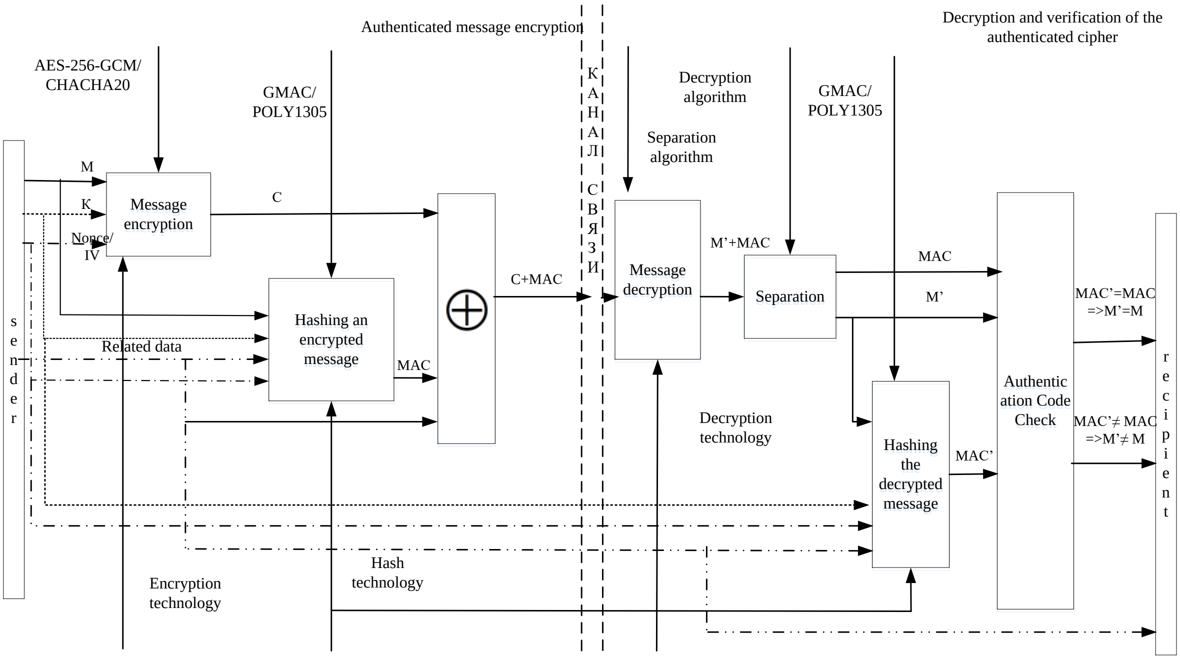

Fig. 3. Scheme of the process of authenticated encryption and authentication of an encrypted message transmitted over a TLS connection

The third process is MAC concatenation and encrypted message (C). The result is sent to the transmission channel and delivered to the recipient (authentication tag). In TLS 1.3, in addition to the encrypted message, related data is authenticated: addresses, ports, protocol version, or sequence number. This information is not encrypted and is known to both parties.

As such, the associated data is also an input to the MAC algorithm, and because of this, the whole process is called Authenticated Encryption with Associated Data, or AEAD for short.

Deciphering an authenticated message and verifying that it has not been altered during transmission consists of four processes.

The first process is the decryption of the encrypted message (C).

The second process is separation. The decrypted message (M') is separated from the authentication code (MAC).

The third process is hashing the decrypted message. The unencrypted message is sent to the MAC algorithm along with the shared secret (K) and nonce/IV.

The fourth process is checking the received hash code. The calculated authentication code (MAC') is compared with the received (MAC) and, if they match (MAC'=MAC), then the received and sent messages match (M'=M).

Thus, the TLS protocol provides both confidentiality and integrity in the transmission of encrypted data.

At this point in time, the current version of the Internet security protocol remains TLS 1.2. But, since work often takes place over a cellular connection, where high latency is possible, over time, a significant slowdown in the spread of the TLS 1.2 protocol began to occur. To replace it, a new version, TLS 1.3, is being put into operation.

The sequence of actions related to the authentication encryption of information (on the sender's side) and its decryption and verification (on the recipient's side) when establishing a communication session in the TLS 1.2 and TLS 1.3 protocols are shown (Fig. 4, 5).

The results of comparing the TLS 1.3 and TLS 1.2 protocols according to the selected characteristics are shown (tab. 3).

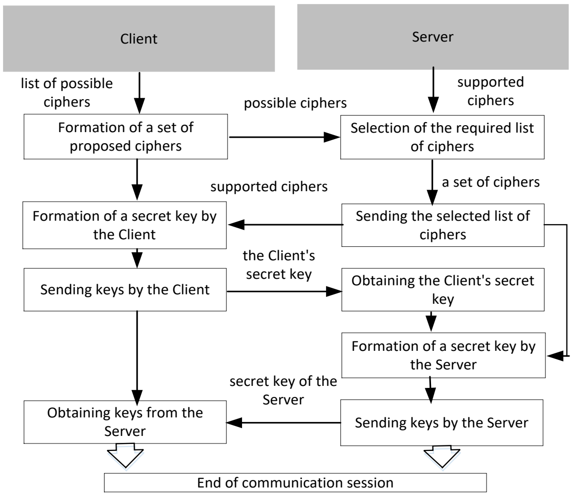
Client
Server
list of possible ciphers
possible ciphers
supported ciphers
Formation of a set of proposed ciphers
Selection of the required list of ciphers
supported ciphers
a set of ciphers
Formation of a secret key by the Client
Sending the selected list of ciphers
the Client's secret key
Sending keys by the Client
Obtaining the Client's secret key
Formation of a secret key by the Server
secret key of the Server
Obtaining keys from the Server
Sending keys by the Server
End of communication session

Fig. 4. Process flow diagram for authentication encryption and decryption using the TLS 1.2 protocol

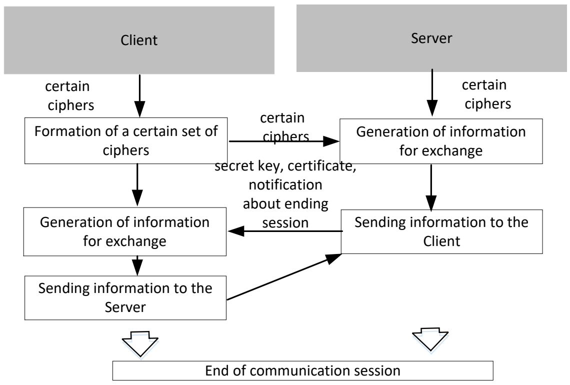
Client
Server
certain ciphers
certain ciphers
Formation of a certain set of ciphers
certain ciphers
Generation of information for exchange
secret key, certificate, notification about ending session
Generation of information for exchange
Sending information to the Client
Sending information to the Server
End of communication session

Fig. 5. Process flow diagram for authentication encryption and decryption using the TLS 1.3 protocol

Table 3

Comparison of TLS 1.3 and TLS 1.2 protocols

Characteristics	TLS 1.3	TLS 1.2
key exchange mechanisms	Diffie-Hellman algorithm or Diffie-Hellman algorithm on elliptic curves; perfect forward secrecy achieved	vulnerable RSA and other static key exchange methods
session end confirmation	one round-trip faster	one round-trip slower
encryption security	AEAD cipher suite - high cryptographic strength	Block Cipher Mode, RC4 or Triple DES - easy to hack
flexibility	key exchange algorithms and signatures are placed in separate fields	key exchange and signature algorithms combined into a cipher suite
number of recommended cipher suites	5 options	37 options
cryptographic signature	more persistent - the whole handshake is signed	less persistent, as part of the handshake is signed
digital signature algorithm	elliptic curve Edwards	RSA
key exchange mechanisms	Diffie-Hellman algorithm or Diffie-Hellman algorithm on elliptic curves; perfect forward secrecy achieved	vulnerable RSA and other static key exchange methods

According to the data presented in Table 3, the following can be distinguished:

1. TLS 1.3 contains more secure key exchange mechanisms, in which only the ephemeral Diffie-Hellman algorithm or the Elliptic Curve Diffie-Hellman algorithm remained. Thus, perfect forward secrecy is achieved, in contrast to the TLS 1.2 protocol;

2. The number of operations for conducting the handshake protocol in TLS 1.3 is at least one round-trip faster than in TLS 1.2;

3. Symmetric encryption in TLS 1.3 is more secure because the set of ciphers used is mandatory, and it also removes some algorithms from the list that are easy to crack, such as Block Cipher Mode, RC4 or Triple DES;

4. The cipher suite in TLS 1.3 is also simpler as it only contains the AEAD and hashing algorithm;

5. Key exchange algorithms in TLS 1.3 and signatures are placed in separate fields, while in TLS 1.2 they are combined into a cipher suite;

6. The number of recommended cipher suites in TLS 1.2 is 37, while in TLS 1.3 there are 5;

7. In TLS 1.3, the signature is cryptographically more secure, since the entire handshake is signed, and not part of it, as in TLS 1.2;

8. TLS 1.3 pays significant attention to elliptic curve cryptography, adding several improved curve algorithms that are as fast as TLS 1.2 without compromising security.

Consequently, the security schemes that exist today, despite their lengthy analysis and research, do not guarantee the same levels of security and stability in the post-quantum period as they do today. This may justify further research in the field of elliptic cryptography using and combining encryption systems with provable security.

Conclusions. The analysis of the current state of the mechanisms for ensuring the reliability and security of data transmission in information and communication systems and networks in the face of modern threats and capabilities of computing technologies allows us to state that it is relevant today to put forward more stringent requirements for ensuring the quality of Internet services. This is justified by the advent of full-scale quantum computers, which can lead to a decrease in the level of stability of symmetric and asymmetric cryptosystems used in modern security protocols.

An analysis of the cryptographic strength of the transport layer security protocols TLS, SSH, IPSec showed that the basis of their strength is symmetric block ciphers that ensure confidentiality, integrity and authenticity. But due to a significant increase in information flows and the spread of digital services, as well as the emergence of a full-scale quantum computer, their stability is questioned, which can lead to a significant increase in the length of key data and a decrease in the level of efficiency. Therefore, it is necessary to consider the feasibility of applying a combined approach to the creation of encryption algorithms.

References

[1]. Service and data availability report, 2023. URL: https: // transparencyreport. google. com / https / overview.

[2]. Guide for Cybersecurity Event Recovery, 2022. URL: https: // nvlpubs.nist.gov / nistpubs /.../ NIST.SP. 800-184.pdf.

[3]. Security requirements for cryptographic modules, 2020, URL: https: // csrc.nist. gov / publications / fips/ fips140-2/fips1402. pdf.

[4]. Guide to LTE Security, 2020, URL: https://csrc. nist.gov / publications / drafts/800-187/sp800_187_draft. pdf.

[5]. S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others, Synergy of building cybersecurity systems: monograph, PC TECHNOLOGY CENTER, Kharkiv, Ukraine, 2021, 188 p.

[6]. O. Tsyhanenko, Development of digital signature algorithm based on the Niederreiter crypto-code system, Information Processing Systems, 2020, Issue 3 (162), pp. 86-94.

[7]. A. A. Havrylova, Analiz kryptografichnyh algorytmiv podanyh do tretyogo turu konkursu NIST, Aktualni pytannia zabezpechennia slugbovo-boyovoii diyalnosti syl sektoru bezpeky i oborony : materialy vseukr. krug. syolu (m. kharkiv, 23 kvit. 2021 r.), FOP Brovin O.V., Kharkiv, Vyp. 5, 2021, pp. 361-365.

[8]. Report on Post-Quantum Cryptography, 2022, URL: https: // csrc.nist.gov / publications / detail / nistir/ 8105/final.

[9]. M. V. Yesina, S. G. Vdovenko, I. D. Horbenko, Modeli bezpeky postkvantovyh asymetrychnyh shyfriv na osnovi nerozriznuvasti, Zbirnyk naukovyh prac GVI,

Kharkiv, Vyp 16, 2019, pp. 15-26. doi: 10.46972/2076-1546.2019.16.02.

[10]. A. Voropay, S. Pohasii, O. Korol, S. Milevskyi, Development of security mechanisms for SCADA systems in the postquantium period, Systemy obrobky informacii, Vyp. 2 (169), Kharkiv, 2022, pp. 25-34. doi: 10.30748/soi.2022.169.03.

[11]. M. V. Yesina, Model bezpeky postkvantovyh protokoliv inkapsuliacii kluchiv, Prikladnaya radioelektronika, 2018, Tom 17, № 3, 4, Kharkiv, pp. 160-167.

[12]. Daniel J. Bernstein Johannes Buchmann Erik Dahmen. Post-Quantum Cryptography, 2020, URL: https: //www.researchgate.net /profile/Nicolas_Sendrier/publication / 226115302_Code -Based_ Cryptography / links / 540d62d50cf2df04e7549388 / Code - Based-Cryptography.pdf.

[13]. Katz, Jonathan; Lindell, Yehuda. Introduction to Modern Cryptography: Principles and Protocols // Chapman and Hall/CRC, 2007, 552 p.

[14]. FIPS PUB 180-4, Secure Hash Standard (SHS), 2019, URL: https: // nvlpubs.nist.gov / nistpubs/ FIPS / NIST.FIPS.180-4.pdf.

[15]. BIKE: Bit Flipping Key Encapsulation, 2022, URL: https: //bikesuite.org/files/v4.1/ BIKE_Spec.2020.10.22.1.pdf.

[16]. Hamming Quasi-Cyclic (HQC), 2020, URL: http://pqc-hqc.org/doc/hqcspecification _2020-10-01.pdf.

[17]. Classic McEliece: conservative code-based cryptography, 2020, URL: https://classic. mceliece.org/nist/mceliece-20201010.pdf.

[18]. McEliece R.J. A public-key cryptosystem based on algebraic coding theory // Prog. Rep., Jet Prop. Lab., California Inst. Technol, 1978. pp. 114-116.

[19]. Post-Quantum Cryptography, 2018, URL: https: // csrc.nist. gov / Projects / postquantum-cryptography / round-3-submissions.

[20]. M.S. Lucenko, Postkwantovyy algoritm inkapsulacii kluchey Classic McEliece, Radiotechnika, Kharkiv, Vyp. 203, 2020, pp. 60-81.

[21]. Alla Havrylova, Yuliia Khohlachova, Volodymyr Pohorelov, Analiz zastosuvannia hibrydnyh kryptokodovyh konstrukciy dlia pidvyshennia rivnia stiykosti hesh-kodiv do zlamu, «Bezpeka informacii», Tom 28, № 2, 2022, URL: https://jrnl.nau.edu.ua/index.php/Infosecurit,doi: 10.18372/2225-5036.28.16953.

[22]. A. Gavrilova, I. Volkov, Yu. Kozhedub, R. Korolev, O. Lezik, V. Medvediev, O. Milov, B. Tomashevsky, A. Trystan, O. Chekunova, Development of a modified UMAC Algorithm based on crypto-code constructions, Eastern-European Journal of Enterprise Technologies, Kharkiv, № 4/9 (106), 2020, pp. 45-63. doi: 10.15587/1729-4061.2020.210683.

[23]. Alla A. Havrylova, Olha H. Korol, Stanyslav V. Milevskyi, Lala R. Bakirova, Mathematical model of authentication of a transmitted message based on a McEliece scheme on shorted and extended modified elliptic codes using UMAC modified algorithm, Кібербезпека: освіта, наука, техніка, No 1(5), 2019, pp. 40-51. doi: 10.28925/2663-4023.2019.5.4051.

[24]. Alla Havrylova, Andrii Tkachov, Rahimova Irada Rahim Qizi. Estimating the Efficiency of Using the Modified UMAC Algorithm // 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), 03-07 October 2022, Kharkiv, URL: https: // ieeexplore.ieee. org/ document / 9916425 / metrics#metrics. doi: 10.1109 / KhPIWeek57572.2022.9916425.

[25]. Serhii Yevseiev, Alla Havrylova, Olha Korol, Oleh Dmitriiev, Oleksii Nesmiian, Yevhen Yufa, Asadi Hrebennikov Research of collision properties of the modified UMAC algorithm on crypto-code constructions, PUBLISHER OÜ «Scientific Route», EUREKA: Physics and Engineering, Tallin, Number 1 (38), 2022.pp. 34-43. doi: 10.21303/2461-4262.2021.002213.

УДК 004.056.7:004.056.9:004.738.5

Гаврилова А., Аксьонова І., Хохлачова Ю., Мілевська Т., Дунаєв С. Обгрунтування вдосконалення протоколів автентифікації в умовах постквантової криптографії

Анотація. *У статті досліджено актуальність питань шифрування конфіденційних даних для їх передачі незахищеними каналами інформаційно-комунікаційних мереж. Проведено аналіз обміну зашифрованою інформацією в мережі Інтернет на базі сервісу Google за обсягом зашифрованого веб-трафіку. Зроблено висновок, що різниця в обсягах трафіку між країнами зумовлена популярністю типів використовуваних пристроїв, інфраструктурою географічного доступу, а також наявністю програмного забезпечення, яке забезпечує сучасні види шифрування. Обгрунтовано роль протоколу HTTPS у забезпеченні безпеки роботи з ресурсами в мережі Інтернет. Проаналізовано вимоги безпеки NIST для сучасних інформаційно-комунікаційних систем у постквантовий період. Визначено, що за короткий проміжок часу потужність обчислювальних пристроїв зростає експоненціально, що тягне за собою збільшення реалізації як уже відомих, так і нових атак на криптографічні алгоритми, які забезпечують надійність сервісів безпеки в мережах. За результатами цього дослідження продемонстровано результати порівняльного аналізу складності класичних і квантових алгоритмів. Розглянуто класифікацію спеціальних атак за ознаками впливу на обчислювальні процеси, за доступом до систем і засобів, а також за специфікою самих атак. Проаналізовано рішення, подані для участі в конкурсі NIST на визначення стандартів безпеки через механізми електронного цифрового підпису, алгоритми шифрування та інкапсуляцію ключів. Результати аналізу представлені у вигляді схеми безпеки та стабільності запропонованих протоколів і алгоритмів. Рекомендується використовувати протоколи TLS для забезпечення цілісності та автентичності користувачів під час встановлення сеансів зв'язку з веб-сайтами. Розроблено схему процесу автентифікованого шифрування та автентифікації зашифрованого повідомлення, що передається через TLS-з'єднання. Розроблено технологічну схему аутентифікаційного шифрування та дешифрування інформації при встановленні сеансу зв'язку в протоколах TLS. Проведено порівняльний аналіз характеристик протоколів TLS 1.3 і TLS 1.2.*

Ключові слова: *NIST, HTTPS, TLS, цифровий підпис, комбіновані алгоритми шифрування.*

Гаврилова Алла Андріївна, доктор філософії, доцент кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут», Україна.

Alla Gavrilova, PhD, associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Аксьонова Ірина Вікторівна, кандидат економічних наук, доцент кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут», Україна.

Iryna Aksonova, candidate of economic sciences, associate professor of cybersecurity department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Yuliia Khokhlachova, candidate of technical sciences, professor of the department of information technology security of the National Aviation University.

Мілевська Тетяна Сергіївна, старший викладач кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.

Tetiana Milevska, senior lecturer of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Дунаєв Сергій Владиславович, аспірант кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.

Sergii Dunaiev, PhD student of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Отримано *2 березня 2024 року*, затверджено редколегією *1 квітня 2024 року*