CRYPTOGRAPHY AND COMMUNICATION SECURITY IN THE DIGITAL AGE

E.I.Saidaxmedov
Denov Institute of Entrepreneurship and Pedagogyi
techmespeaker@gmail.com
Z.O.Nurmatov
Denov is a teacher at the Institute of Entrepreneurship and Pedagogyi
nurmatovzohidjon35@gmail.com
G.T.Doniyorova
Denov is a teacher at the Institute of Entrepreneurship and Pedagogy
gulshandoniyorova68@gmail.com
https://doi.org/10.5281/zenodo.8251415

ANNOTATION Have you ever forgotten your password on a website you signed up for months ago? This password recovery process begins with a trial and error process of familiar passwords and is usually followed by a "Forgot Password?" ends by pressing the button. button nearby. When you refresh your inbox in search of an email the website sent you, the instructions to log in to your account will finally arrive. Here's a red flag: this email contains your old password in plain text. If you do, you should question the security of this website and consider deleting your account.

Key words: cryptographic, symmetric key cryptography, public key cryptography, encryption, quantum computers, quantum cryptography.

Internet security is becoming an increasingly important issue in this digital age, especially as we store exponential amounts of personal and personal information online. Here's a helpful tip: never store your passwords in plain text. Doing so increases the risk of compromising the security of online databases and, perhaps more importantly, your personal account information. hacked the database, they would immediately have access to a number of accounts. This is where the importance of cryptography, or rather encryption, to create secure data systems comes into play.

Cryptography is the science of securely transferring information from one source to another. You may not notice the daily use of cryptography in your life, but its importance cannot be understated. Today, cryptography is widely used in communication and payment systems such as e-commerce websites, mobile phones, credit cards, and computer passwords. The goal is to prevent third parties from accessing personal information. Today, thanks to cryptography and the ability to create secure means of data transfer, sensitive information such as bank account details or social security numbers can be entered online. As theft becomes more sophisticated, cryptography becomes one of the most important security measures in protecting personal information.

Principles of cryptography

Cryptography has three main purposes to ensure security. The first of them is data integrity. When messages are sent between two sources, the recipient of the message must be able to distinguish whether the message has been tampered with or not. In other words, the receiver must be able to determine whether a certain part of the message is forged or not. The second purpose of ensuring secure communication is authentication. When the message is received, the receiver must verify the identity of the sender. Finally, cryptography is used to

strengthen non-repudiation. is also focused, meaning that once a message is sent, the sender cannot deny that he is the original author [4]. Successful cryptography must achieve all of these goals: integrity, authentication, and non-repudiation. Written with pen on paper For messages, these goals are relatively easy to achieve because private signatures are a means of verifying the original author and their intent. History of cryptography The practice of cryptography has been around for centuries, with examples of message encryption dating back to 1900 BC in Egypt. The Atbash cipher was used to encrypt Hebrew messages by changing the first letter of the Hebrew alphabet to the last letter, the second letter to the second letter to the last letter, and so on until the alphabet was effectively reversed.[1].

A cipher is a set of instructions for encrypting a message, and a "key" is an instruction on how to effectively open and read the message. One of the most famous examples of cryptography was what is known as the Caesar cipher. Julius Caesar o encrypted his messages to his generals using a permutation cipher in which each letter of the alphabet was shifted a certain number of positions. entrusted them with the key to the solution. For example, the word "cryptography" is written as "fubswrjudskb". Here, the key is 3 and indicates the replacement cipher with a shift to the 3rd letter after it. Each arrow shows the corresponding letter in the transposed alphabet. With the advent of computers and the digital age, basic ciphers and encryption methods are no longer the most successful means of protecting information. Computers allow brute-force methods that make ciphers, such as the Caesar cipher, very fragile. In the 1970s, The United States government found it necessary to create a standard for encrypting classified information. A group of IBM researchers found a solution to the government's needs by creating an algorithm for encrypting data using symmetric key cryptography. Symmetric key cryptography Symmetric key cryptography is a basic form of cryptography that involves the exchange of messages between two parties. First, the two parties agree on a key to use for encrypting and decrypting the messages. Before sending a message to party B, party A uses an encryption algorithm and both parties encrypt this message using an agreed upon key. After party B receives the encrypted message, they use the key to return the ciphertext to plaintext. This type of cryptography is called symmetric key cryptography because both parties to the communication have the same encryption and decryption key. they use the same key [4].

Symmetric key encryption provides a very fast and efficient way to encrypt messages, but it has several security flaws. The key to decrypt a message must be shared securely with both parties before the message is sent. If an attacker has access to the key, they could easily encrypt each party's messages. Because of its speed, symmetric-key encryption is useful for encrypting large amounts of data. The problem with symmetric-key encryption is how to securely share the key. This shortcoming led to the creation of public-key cryptography 40 years later. Public key cryptography Unlike symmetric key cryptography, as the name suggests, public key cryptography uses a public key to encrypt data. In a public key encryption system, each communicating party has a pair of keys. The public key used to encrypt messages can be distributed to anyone. , and the user's private key must be kept secret. In this system, if party A wants to send a secure message to party B, party A first encrypts its message using party B's public key. The only way to encrypt a message using party B's public key is is to use B's private key. A step-by-step process of public-key encryption, demonstrating the use of different keys in the encryption/decryption steps.[6]

An example of public key cryptography is Transport Layer Security (TLS). TLS provides confidentiality and data integrity between a client (such as your web browser) and a server (such as amazon.com). when connected, data is encrypted using symmetric key cryptography before being sent. The client and server agree on which key to use before transmitting any data. The identities of both parties are then authenticated using public key cryptography [7]. you can see when TLS is being used. If you see a web address starting with "https", you know your data is secure. Encryption methods, such as symmetric or public key cryptography, are designed to be reliably secure. That is, it can be mathematically proven that a cryptographic algorithm resists certain types of attacks. The security of an algorithm is usually based on several assumptions about the attacker's capabilities. , the attacker does not have unlimited computing power, and some basic assumptions in mathematics remain true. One of the most widely used public-key cryptographic algorithms, RSA, relies on the idea that the prime factors of large integers cannot be computed. Therefore, when calculating the security of RSA, it is assumed that the attacker is not capable of performing such a task. The Future of Cryptography and Encryption.

Cryptography constantly tries to stay ahead of attackers to provide a secure way to transmit data. As computers become more powerful, cryptographic algorithms become sophisticated enough to make brute-force decryption attempts infeasible. Quantum cryptography has been proposed to solve the security risk of key sharing in symmetric key cryptography. Quantum mechanics can be used to generate a key to encrypt data as in ordinary computing. However, unlike conventional encryption keys, a quantum system can be measurement disturbs the system. If an attacker tries to read the key while it is being generated, the system stops communication attempts [8]. This theoretically provides absolute security in communication, since symmetric keys can be shared without fear of being intercepted by a hacker. can be seen. Quantum computers and quantum cryptography are still in research; it will be many years before quantum technology is widely used. As quantum computers move closer to technological reality, the future of cryptography will focus on creating systems resistant to quantum computer attacks.

Summary

It's easy to overlook the impact of cryptography on protecting our data. Not so long ago, consumers couldn't buy things online or check their bank statements from their home computers in the "next century." The introduction of advanced cryptography and security protocols like HTTP has made the World Wide Web a much safer place to share sensitive information. It may be some time before cryptography provides absolute security; however, the field of cryptography has made great strides in creating secure communication methods over the past few decades. E-commerce websites, mobile phones, credit cards and password security innovation have evolved with cryptography. Time will tell what new inventions cryptography will lead to.

References:

[1]BM Metzger and MD Coogan, The Oxford Companion to the Bible. Oxford[et al]: Oxford University Press, 2004

[2]S. Vodenay, A Classic Introduction to Cryptography: Applications to Communication Security.New York: Springer-Verlag New York, 2005
[3]P. Thorsteinson and GAG Ganesh, .NET Security and Cryptography. United States: Prentice Hall PTR, 2003.
[4]H. Delfs and H. Knebl, Introduction to Cryptography: Principles and Applications, 3rd ed. 2015.
[5]K. Krishnan, "SFWR 4C03: Computer Networks and Computer Security", North Carolina State University, 2004.
[6] “Public Key Encryption”, www.tutorialspoint.com, 2016. [Online].Available at: http://www.tutorialspoint.com/cryptography/public_key_encryption.htm. Entered: September 7, 2016.
[7] T. Dierks, "Transport Layer Security (TLS) Protocol Version 1.2", 2008. [Online]. Available at: https://tools.ietf.org/html/rfc5246. Entered: September 8, 2016.
[8] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nature Photonics, vol. 8, no. 8, pp. 595–604, July 2014.
[9] Islomovich, S. E. (2023, March). MAVZU: ELEKTRON RAQAMLI IMZO VA BULUT TEXNOLOGIYALARI: FOYDALANISH MASALALARI TAHLILI. In Proceedings of Scientific Conference on Multidisciplinary Studies (Vol. 2, No. 3, pp. 31-34).
[10] Saidahmedov, E. (2023). KVANT ALGORITMLARNI ISHLAB CHIQISHDA KVANT KOMPYUTERLARINING O ‘RNI. Наука и инновация, 1(1), 58-64.
[11] Islomovich, S. E. (2023, May). THE ROLE OF QUANTUM COMPUTERS IN THE DEVELOPMENT OF QUANTUM ALGORITHMS. In INTERNATIONAL SCIENTIFIC CONFERENCES WITH HIGHER EDUCATIONAL INSTITUTIONS (Vol. 1, No. 05.05, pp. 557-563).
12.Nurmatov, Z. O., Tursunpulatova, K. A., & Nasriddinova, Z. N. (2023, May). THE ROLE OF MULTIMEDIA TECHNOLOGIES IN TEACHING FOREIGN LANGUAGES. In International Conference on Science, Engineering & Technology (Vol. 1, No. 1, pp. 99-103).
13.Якубов, С. Х., Хамраев, А. А., Хушбоков, И. У., & Нурматов, З. О. (2022). АЛГОРИТМИЗАЦИЯ САПР ОПТИМИЗАЦИИ ТОНКОСТЕННЫХ ЭЛЕМЕНТОВ ИНЖЕНЕРНЫХ КОНСТРУКЦИЙ. Universum: технические науки, (11-1 (104)), 53-59.
14.Shamsiddinovich, M. R., & Obidjonovich, Z. N. (2021). Advantages and Improvements of E-Textbook Teaching of Computer Science in General Secondary Educatin. CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES, 2(12), 71-74.
15. Nurmatov, ZO, Chorshamiyeva, ON, & Pirimova, F.A. (2023). KIBERXAVFSIZLIKNI TASHKIL ETISHDA AXBOROT TEXNOLOGIYALARINING ROLI. TA'LIM VA RIVOJLANISH TAHLILI ONLAYN ILMIY JURNALI , 3 (5), 432-442.