Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 24-27 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

KEY IN CRYPTOGRAPHY AND THEIR IMPORTANCE FOR SECURITY

გასაღები კრიპტოგრაფიაში და მათი მნიშვნელობა უსაფრთხოებისთვის

მაქსიმ იავიჩი - კავკასიის უნივერსიტეტი

Maksim Iavich – Caucasus University

საბა ჩალაძე. N192 საჯარო სკოლა

Saba Chaladze. N192 public school

დავით ღელაღუტაშვილი. N199 საჯარო სკოლა

Davit Ghelaghutashvili. N199 public school

დაჩი გრძელიშვილი.

Dachi Grdzelishvili.

ალექსი ბერიშვილი. N199 საჯარო სკოლა

Aleksi Berishvili. N199 public school

თორნიკე კუმელაშვილი. N199 საჯარო სკოლა

Tornike Kumelashvili. N199 public school

საკვანძო სიტყვები: *კრიპტოგრაფია, გასაღები, უსაფრთხოება*

KEYWORDS: *cryptography, key, security*

აბსტრაქტი: აღნიშნულ სტატიაში, ჩვენ გავეცანით გასაღების გამოყენების ძირითად პრინციპებს კრიპტოგრაფიაში და მის მნიშვნელობას უსაფრთხოებაში. ჩვენ, ასევე, მიმოვიხილეთ RSA ალგორითმი, რომელიც გამოიყენება თანამედროვე კომპიუტერებში, შეტყობინების დაშიფრვისა და განშიფვრისათვის.

ABSTRACT: In this paper, we went over the basic principles of key usages in cryptography and its importance in security. We also reviewed the RSA algorithm, which is used by modern computers to encrypt and decrypt messages.

INTRODUCTION

Encryption is a process that encodes a message or file so that it can be only be read by certain people. Encryption uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information. The message contained in an encrypted message is referred to as plaintext. In its encrypted, unreadable form it is referred to as ciphertext.

Basic forms of encryption may be as simple as switching letters. As cryptography advanced, cryptographers added more steps, and decryption became more difficult. Wheels and gears would be combined to create complex encryption systems. Computer algorithms have now replaced mechanical encryption.

What is an encryption key

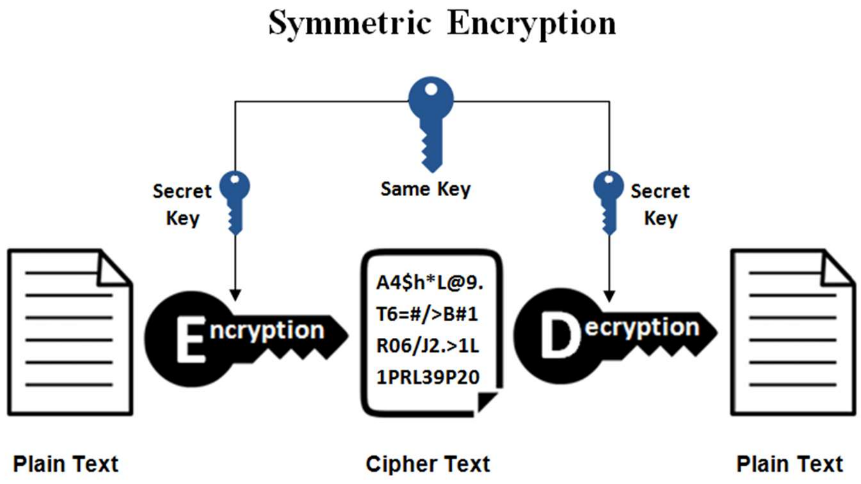
An encryption key is typically a random string of bits generated specifically to scramble and unscramble data. Encryption keys are created with algorithms designed to ensure that each key is unique and unpredictable. The longer the key constructed this way, the harder it is to break the encryption code.

Two types of encryption algorithms can be used by the encryption key server: symmetric algorithms and asymmetric algorithms.

Symmetric-key encryption

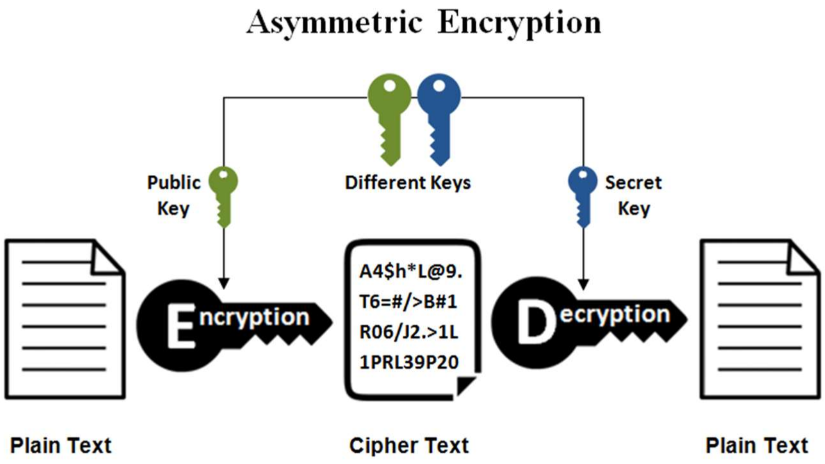
Symmetric-key algorithms use the same keys for both encryption and decryption. The keys may be identical or there may be a simple transformation to switch between the two states. The Caesar and ROT13 ciphers above both use a symmetric-key.

The key acts as a shared secret between two (or more) parties that can be used to send private information that cannot be read by anyone without a copy of the key. The main drawback here is the chicken and egg problem of sharing the secret key. Without a secure channel the key cannot be shared, but without the key no secure channel can be created. In times past this meant meeting in the real to swap a physical copy of the key, the only way to secure against anyone listening in. However, in 1976 a new method was published, allowing this to be done securely online.



Asymmetric-key encryption

Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that only you know. A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.



RSA Algorithm

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name RSA algorithm.

RSA works by generating several different encryption keys.Two of those encryption keys are based on large prime numbers.Some math is done on these prime numbers using a one-way function — a mathematical operation that is easy to perform but which cannot be reversed if the answer and only some of the starting information is known. This gets a shared value which allows one of the prime numbers and it to be distributed as a public key, and one of the numbers and it to be kept secret and used as the private key.

Messages encrypted with the private key can easily be decrypted by the public key, which demonstrates that the person who did so holds the private key. This is used for signing messages.

Messages encrypted with the public key can only be decrypted by the private key — this allows the encrypted message to be transmitted over unsecured methods.

Key Security's Importance

Why is key security so important? To explain, let's look at a fundamental principle of cryptography, the so-called Kerckhoff's principle. According to this, security of a cryptosystem is not dependent on the security or confidentiality of any of its parts, but on the key(s) and the key(s) only. Consequently, a communication security problem is essentially a key management problem, as maintaining key security falls into the very definition of key management. Thus, good design of a cryptosystem, which should basically guarantee the complexity of its security, should eventually boil down to the efficient protection of a few cryptographic keys. There are three elements into which key security is divided:key confidentiality or key secrecy, key authenticity or verification of key sender identity, authorized use of the key or permissible use of the key

Cracked: 30 Year-Old Cryptography System

Dublin City University (DCU) researchers, Neill Costigan, PhD student at DCU and funded by the Irish Research Council for Science, Engineering and Technology (IRCSET) and Prof Michael Scott member of the Science Foundation Ireland (SFI)-funded Shannon Institute of Cryptography, have successfully cracked a crypto system published thirty years ago by coding theorist Robert J McEliece.

The crack which was accomplished using resources at the SFI-Funded Irish Centre for High End Computing was announced at the Post-Quantum Cryptography conference in Cincinnati, USA on Saturday 18 October.

Quantum computers will break current public key algorithms such as RSA. McEliece's system is not affected by quantum computers and is a leading candidate for future public-key cryptography. The successful attack shows that the originally proposed key sizes for McEliece's system are too small and need to be increased.

The DCU success was part of a coordinated attack by cryptographers in five countries. The attack was led by Prof Tanja Lange and Christiane Peters (Eindhoven Technical University, TU/e) and Prof Daniel J Bernstein (University of Illinois at Chicago), who recently published a paper claiming that a practical attack on McEliece's system was feasible with their new software.

Costigan and Scott ran the software at ICHEC for 8000 CPU hours and achieved the first break on Wednesday 2nd October 2008. Other countries ran the software for a total of 200000 CPU hours but did not have the luck of the Irish.

Acknowledgement

The work was conducted as a part of SPG-19-133 financed by Shota Rustaveli National Science Foundation of Georgia.

REFERENCES:

1. What is Encryption & How Does It Work? medium.com 2017.
2. T.Anton, The need to manage both symmetric and asymmetric keys, cryptomathic.com. 2019
3. Giorgos-Nektarios Panayotidis, The Role of the Key in Cryptography & Cryptosystems, study.com
4. Symmetric vs. Asymmetric Encryption – What are differences?, ssl2buy.com
5. M Iavich, G Iashvili, A Gagnidze, L Nachkebia, S Khukhashvili, THE ANALYSIS OF THE DIFFERENCE OF 4G AND 5G SECURITIES, Scientific and practical cyber security journal