VOLUME: 3
ISSUE: 3
SEPTEMBER - DECEMBER, 2019
PRIZREN SOCIAL SCIENCE JOURNAL
ISSN: 2616-387X
DOI: 10.32936/PSSJ.V3I1

ENCRYPTED DATA SERVICE FOR SECURITY ELECTRONIC COMMUNICATIONS

Prof. Asoc. Dr. Naim BAFTIU

Dr. Sc. Ahmet NUREDINI

Prof. Asoc. Dr. Samedin KRRABAJ*

**Correspondent Author: University of Prizren "Ukshin Hoti", Faculty of Computer Science, samedin.krrabaj@uni-prizren.com*

Article history:

Accepted 01 September 2019
Available online 31 December 2019

Keywords:
Communication
security
electronic privacy

Abstract

The law on electronic communications has so far enumerated a considerable number of natural persons, legal entities as well as public institutions that use code systems and crypto devices during communication. Of particular interest is addressing the key role of operators and providers of encrypted data services in combating abuses committed through or against computer systems as the responsible performance of their duties to protect the security of networks and computer systems affects significantly in controlling illegal risks and attacks. In this perspective, the specific legal obligations for the protection of privacy regarding personal data that are processed for the purpose of providing information services are also analysed.

The purpose of the paper is, utilizing communication between two parties sharing a common key, implementing a shared key to protect data communicated with different security attributes, Role of cryptography in data protection during communication, and Focus on privacy. Of the data communicated, against their authenticity.

Introduction

Cryptography is very important for transferring information from one place to another, and not wanting anyone to read it. With the rapid growth of internet use and all the work being done on it, such as online banking, which is directly related to our money, the need for electronic security is increasing.

Cryptography is used to enhance the security of online communication such as e-mail messages, online transactions, computer passwords, ATM card transactions, computer data and many other private information.

1. Symmetric Crypto - Classic Definition

Cryptography is an uncommon science, a scientific discipline that deals with the discovery and advancement of methods for converting open text into digits and figures into open text. In this science, research culminates only when the result provides the confidential information to unauthorized persons, regardless of how they are exchanged. The notions of cryptography, with the notion of open source, mean information dedicated to one or more collaborators involved in the unique communication system. By the notion of digits, we mean the incomprehensible (encrypted) text for unauthorized persons not found in the unique system of secret communication. By the notion of decoding we mean the reverse coding action, by which we know the encryption-decoding method to convert the cipher into open text (Hamit 2011).

If the cipher is transmitted to the receiver, in the hands of unauthorized persons it is called a cryptogram. The action to open that cryptogram without knowing the encoding-decoding method is called Decryption. By key notion we mean the secret word (password) which roughly defines the way of deciphering. In cryptography the key will play a crucial role in determining the cryptographic value of a system. The encryption is done by applying certain methods, which should be known only to the sender and receiver of the secret information. Only in this way can the sender and the recipient exchange information, the confidentiality of which is guaranteed. The advantage of encrypted information is that even if it falls into the hands of unauthorized persons, they will understand nothing from non-information (Hamit, 2011).

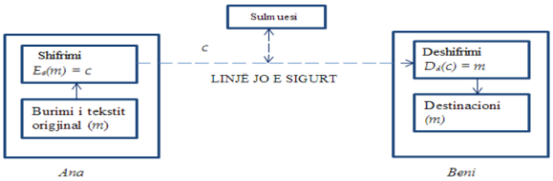


Figure 1. scheme Basic communication

The symmetric encryption scheme has five components:

•**Plain Text** - The original or original message to be sent is known as open text.

•**Cipher Text** - The message on which the cipher is applied is known as the cipher text.

In cryptography the initial message "hello" can be converted to such incomprehensible form "**Ajd672 # @ 91uk**".

Encoding - The process of converting an open text into encoded text is known as encoding. Cryptography uses encryption techniques to send confidential messages over an unsecured line of communication. The coding process requires two things: a coding algorithm and a key. The encryption algorithm means the technique used and the encryption occur on the sender side.

•**Decoding** - An inverse process of decoding is known as decoding, where the encoded text is converted to the original text. Cryptography uses decoding techniques on the recipient's side to retrieve the original message from the encoded text.

•**Key** - A key is an alphanumeric text or may be a special symbol.

A source produces a message clearly, e.g. **X = [X1, X2... XM].**

A key of the form **K = [K1, K2... KJ**] is generated.

If the key is generated at the message source, then it must also be secured to the destination via a secure channel.

Alternatively, a third party may generate the key and deliver it to the source and destination. The cipher text **Y = [Y1, Y2... YN]** is generated by the encryption algorithm with the **X** message and the **K** encoding key as input. The Encryption Process is: **Y = E (K, X)**

This notation indicates that **Y** is produced using the encryption algorithm **E** as a simple function **X**, with the specific function defined by the value of the key **K**. The target key receiver is able to reverse the transformation according to the formula: **X = D (K , Y)**

An opponent, observing Y but not having access to K or X, may attempt to cover **X** or **K** or both. It is assumed that the opponent knows the encryption **(E)** and decryption **(D)** algorithms.

The opponent can do one of the following. Remove **X** by generating a simple **X** ^ rating, if the opponent is only interested in this particular message Recover K by generating a **K** ^ rating, if the opponent is interested in being able to read future messages.

There are several terms associated with cryptosystems:

- Cryptologist
- Cryptography
- Cryptanalysis and
- Cryptosystems:

Cryptosystems - A cryptographic system or a cryptosystem is a system that enables two parties to communicate securely. A cryptosystem contains five elements (**Ƥ, C, K, E, D**), each of which is described as follows:

Ƥ - Represents a finite set of possible initial texts,

C - A finite set of possible coded texts,

K - A finite set of possible keys,

E - A set of cipher functions,

D - A set of corresponding decoding functions.

Mathematically a cryptosystem is defined as follows: Definition: Let Ƥ be the open text space, C the encoded text space, **K** the space of the keys. Let c be the decoding function and **dk** the decoding function.

Then for each key **k ϵ K**, there is a decoding function and a corresponding decoding function such that **dk (ek (x)) = x** for each element **xϵ Ƥ**. Each function must be injected able as the decoding must be unique.

There are three types of cryptography forms:

1.Hidden Key Cryptography (DES, IDEA. AES)

2.Public Key Cryptography (RSA, DSS, PGP, ECC)

3.HASH Algorithms (SHA, MD2, MD4, MD5)

Security components:

1.Confidentiality of data that provides private data, which is not disclosed to any unauthorized user.

2.Data integrity ensures that programs and data are changed only in a specified and authorized manner. System integrity ensures that the system performs its function without damaging anything, free from unauthorized manipulations.

3.Availability ensures that systems work safely and service is not denied to the automated user.
(Confidentiality, Integrity and Availability) - CIA.

Additional concepts: Authenticity: the property of being true, trustworthy, and capable of being verified. Responsibility: the requirement for an entity's actions to be uniquely traced to that entity.

Security Aspects: Aspects of information security
1.Security attacks - any action that endangers the security of information owned by an organization.
2.Security Mechanism - A process designed to detect, prevent a security attack.
3.Secure services - the security of data processing systems, transfers of an organization.

1.1. The Importance of Securing Data Encrypted During Communication

In some cases the decoding or decoding transforms are characterized by keys and if they are discovered by someone it will not be necessary to design a scheme from scratch but simply switching the key would be enough. Frequent switching of the key is in fact considered a genuine cryptographic practice. An indispensable but usually not sufficient condition for the security of a cipher is related to the fact that the key space is large enough to render exhaustive search impossible.

What is worth noting is that the size of the key greatly affects cryptography. Almost most asymmetric schemes allow for **1024-bit** keys and more, even according to Shamir, the **512-bit** keys in the RSA "protect 95% of online E-commerce nowadays".

Where asymmetric systems are used in the exchange of symmetric keys, the lengths of the public keys are chosen to be resistant to certain specific levels of attack. The length of the secret keys exchanged in the system must be such that it has a level of resistance to a given attack. Thus, the three parameters - the strength of the system, the strength of the secret key, and the strength of the public key must coincide with each other.

This is more widely discussed in RFC 3766 with respect to determining the strength of public keys used in the exchange of symmetric keys. If we consider the size of the keys in the cryptography of the elliptical lines, they turn out to be much smaller than the **RSA** keys. Consequently we have faster processing and less memory and bandwidth requirements. Some studies find that Elliptic Curve Cryptography (ECC) is faster than **RSA** for signature and decoding, but slower for signature verification and encryption. A 256-bit **ECC** key is as secure as a 3248-bit key in the RSA algorithm.

Table 1. Key length for RSA security

The length of the key	Potential categories for finding the key
256 bit	Potential categories for finding the key
384 bit	Scientific research groups (University) and cryptographic communities
512 bit	Governments
768 bit	Safe in a short period
1024 bit	Safe for the near future
2048 bit	Safe for decades?

1.2. Communication control

There are various algorithms that encrypt information. The greater the number of bits using such key algorithms, the more secure the encryption will be. If e.g. the 32-bit algorithm is used, the number of possible combinations per key is **2 ^ 32 (4294967296)**. For small companies and most universities, the 40-bit algorithm is used.

The safest algorithms used utilize 128 bit encryption, with which **(340.282.366.92.938.368.736.424.720.624.720.032.456)** key combinations are achieved. So it is very difficult to get into the system and break down such security. Because to break such information one has to try so many combinations in sequence! Technically impossible to achieve, even with the simultaneous operation of 1 million processors!.

Recent studies, conducted by independent researchers, have shown that a key with a length of not less than 90 bits guarantees complete security for the next 20 years.

The algorithms used to calculate the values of private keys d by public keys e and technology change over time. Thus the calculation of **Wd** can result in different values. Concerning the security of a cryptosystem there are concepts of information theory which we will see in the following chapter. The Kickoffs principle and the Shannon principle are among the most popular assumptions in cryptanalysis. In fact, the safest cryptographic algorithms are those algorithms that, being publicly known and constantly subject to cryptanalysis, continue to resist and qualify as unbreakable. The 20th century, and especially the two world wars, took cryptography to new sophisticated levels, using sophisticated coding machines like the German "Enigma" that resembled a typewriter. When the operator typed normal text, some electronically connected rotors encrypted the message. The encrypted text was then sent in Morse code and decrypted by another Enigma machine. However, the errors and carelessness of the redundant operators gave important data to the code breakers, enabling them to decrypt the messages.

In today's digital world, banking, money transfers and various payments, as well as medical, corporate and government data, are provided with complex encryption.

The encrypted text is then read by those who have the decryption key needed to restore the data to its original form.

2. Modifying S boxes in AES and Bluefish

Static and dynamic boxes- Modifying S boxes can be accomplished thanks to different methodologies in cryptographic algorithms. Before studying these methods let's look at the construction of S. boxes S boxes can be constructed in two separate ways: static and dynamic. In the static boxes, the values of the input vectors are not changed while in the dynamic boxes their values will be changed.

The following are the views of the S boxes in both cases:

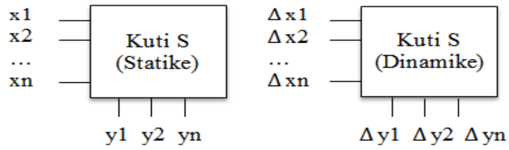


Figure 2. Static and Dynamic S boxes

The properties of the boxes in each case are determined using a specific metric such as entropy, which estimates how random the data are, denoted by **H (Z)** and given as a random variable 'z' (Rodwald and Piotr Mroczkowski, 2006):

$$(Z) = \Sigma P\ ni = 1\ (Zi)\ \log 2\ (Zi\ -1)$$

The larger the entropy, the harder it is to replace the values. Many of the encryption algorithms use static or dynamic boxes. The boxes in **DES** are static and resistant to differential cryptanalysis but if we use certain methods to give them a dynamic nature this would obviously increase their nonlinearity. The Camellia algorithm has the Avalanche feature and every element of the S boxes in it is polynomial in GF (28) making this algorithm robust against high-order differential attacks. Only that Integral attack would be carried out very easily against **128-bit** Camellia (**10/11** rounds) (Zhang et.al., 2013) .

In AES, static replacement boxes define Sub Bytes transformation that provides nonlinearity and confusion in the figure, thanks to multiplicative inverse functions and affine transformation. But at the same time static values make it easier to perform mathematical attacks on AES and this algorithm turns out to be non-resistant to Timing and Cache attacks.

The Bluefish algorithm uses key-dependent dynamic S boxes and is not endangered by linear and differential cryptanalysis methods. But the Bluefish algorithm turns out to be weak against the Vandenay attack. This attack is due to the presence of weak keys in the figure and this is due to the encounter of the same values in the S boxes in Bloopfox, so we can easily apply the attack with the original text selected. In conclusion we can say that dynamic boxes manage to provide more diffusion than static boxes.

Modifying S boxes to make them dynamic can be accomplished by using chaotic equations of random nature. One of them is the Logistic map equation which has the following form (Xin-je, 2009) :

$$Xn+1 = r^*\ Xn\ (1-Xn)$$

Xn takes values from **0 to 1**, r is a positive number from **1 to 4**. In this way a dynamic key dependent S box can be created. The following algorithm can be used for this and changes to the key mentioned in the equation can be applied:

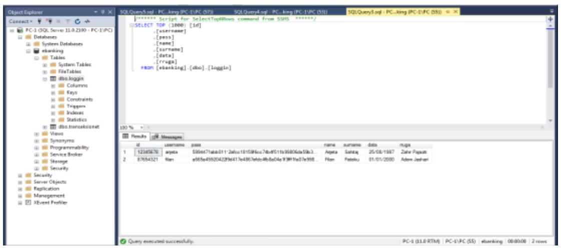
```
for (i=0; i<=dsize; i++)
{
temp=a;
p=k1*(dsize-i);
k1= k2*(1-k2) + (k3/p) + (k4/p);
k2=temp;
System.out.println(a);
V=afterDecimal(k1);
System.out.println(V);
x=V%MDv;
System.out.println(“” + x);
}
```

The only problem with creating S boxes in this way is encountered in repeating values within S boxes (usually no more than **5% to 10%**), but this is resolved by replacing multiple values with others. The security provided by dynamic boxes is commensurate with the values of **DMv** (dependent modulo) and size (S box size). Increasing these values affects the overhead needed by an exhausted attacker to break our cipher. Dynamic boxes are prioritized over the S boxes mentioned above in relation to their operation in key algorithms such as **AES**, Bluefish, etc.

2.1. Security Application

SQL (Structured Query Language) is a computer language designed for data management in relational database management systems, and originally based on relative algebra.

C # (read "as sharp") is a modern programming language for developing software applications. C # is a simple object-oriented language that has roots in the C family of programming languages, which means it is easily understood by the programmers of C, C ++, and JAVA.



```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP (1000) [id]
      ,[username]
      ,[pass]
      ,[name]
      ,[surname]
      ,[data]
      ,[rruga]
  FROM [ebanking].[dbo].[loggin]
```

	id	username	pass	name	surname	data	rruga
1	12345678	arjeta	[illegible]	Arjeta	Sahitaj	25/08/1997	Zahir Pajaziti
2	87654321	Ilan	[illegible]	Ilan	Fetaku	01/01/2000	Adem Jashari

Query executed successfully.

SQLQuery5.sql - PC...king (PC-1\PC (57))
SQLQuery4.sql - PC...king (PC-1\PC (53))
SQLQuery3.sql - PC...king (PC-1\PC (55))
Results
Messages
100 %
PC-1 (11.0 RTM)
PC-1\PC (55)
ebanking
00:00:00
2 rows

Figure 3. Overview of the SQL Server Studio computer language

Microsoft Visual Studio supports various programming languages through the language service, which allows the code editor and debugger (scripting program) to support almost any programming language, ensuring that specific language services exist.

Hash Functions are mathematical functions used to encode notes in a computer. These functions, unlike encryption algorithms, have no encryption or decryption keys. MD5 divides messages into 512-bit blocks

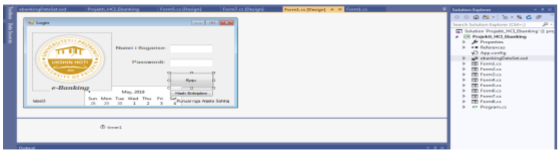


Figure 4. View from the Microsoft Visual Studio programming language

E-Banking Modules:
-Emphasis
-Deposit
-Transfer

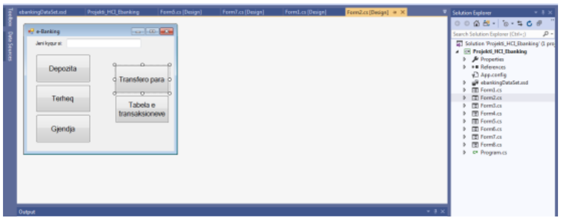


Figure 5. E-Banking Modules

To protect this communication between Databases we have used Encryption to prevent third parties from intercepting them.

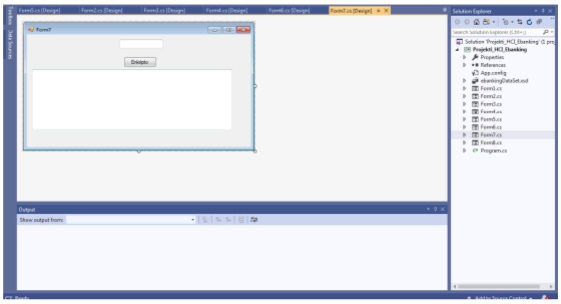


Figure. 6. System Encryption

2.2. Legal-Criminal Characteristics of Offenses Related to Cybercrime, According to the Criminal Code of Kosovo

In the Republic of Kosovo, cybercrime-related offenses are not provided by a single code or law, but are dealt with in some laws. Some of them are foreseen in the Criminal Code of Kosovo, others in the Law on Prevention and Fight against Cybercrime, while such a provision is provided in the Criminal Code, the Law on Classification of Information and Security Verification. We think that such a picture, which is found in the Kosovo legislation, represents a bad legislative practice that needs to be regulated. The solution is to include all criminal offenses of this nature in a separate chapter in the Kosovo Criminal Code.

Given their features and features, cybercrime-related offenses can be understood as any activity in which computers or networks serve as tools or objects of attack for the exercise of criminal activity, against which all appropriate preventive legal measures to combat them. The main characteristic of cybercrime-related offenses is their global effect. For this reason, an international focus is required, as the perpetrators of these crimes are consuming and using various methods that are not confined to specific territorial units when consuming these offenses. They may operate in one place, while the object of their crime, the victim, may be in another. Such offenses include: unauthorized access to computer systems, illegal interception of computer data, interference with computer data, interference with computer systems, abuse of computer equipment, spread of viruses and other actions that endanger computer programs.

2.3. Hacking

Hacking means the human mind against the computer. It is carried out by specialized people, called hackers, who deal with cyber-attacks. Hackers have often made a fuss in fictional accounts as people who stealthily manipulated a maze of computer networks, systems, and data to find and access information. A hacker often spends hours examining the types and structures of the systems he intends to infiltrate, using his deception, fraud, and bypassing controls placed on someone else's proprietary information. They build software programs and use them to accomplish their goals. Expert hacker is usually the master and master of several programming languages, protocols, networks, and operating systems. Also, he skillfully manages to fully master the technical environment of the target computer system. After choosing a system as the target, the likelihood that the expert hacker will successfully enter that system is high.

Cybercrime of hacking is characterized by unauthorized interference with foreign computer systems, which in the classical sense means violent interference with foreign objects (Vula, 2010: 102). In practice there are two ways to accomplish this work. The first involves obtaining the necessary information, with different methods and techniques for successful intrusion into foreign computer systems, such as internet addresses, phone numbers, identifiers, encrypted messages, operating systems, etc. Preliminary information pertains to researching classical emails, newsletters, eavesdropping, false presentations, etc. (Petrovic, 2000: 118). The second way is based on the principle of "try, make a mistake, put away the mistake". In this way the attacker attempts to intrude on the defensive parameters, for infiltration of the particular information system. The perpetrators of this action are the hackers.

2.4. Phishing

Phishing is one of the oldest cybercrime. The idea of the authors of this work is to pretend to be a trustworthy subject on the Internet, trying to get personal information. We are dealing with an email fraud method. The fraudster sends out e-mails that look like official, in search of potential victims, to collect personal and financial information. It is also known that such scams are also used to steal valuable information, such as passwords, credit card numbers, social security numbers, and bank account numbers. During this process, their users, victims, are asked to visit a website to update their personal information via email. Clearly phishing is any process designed to extract personal data from the targeted victim. This is often done by e-mail. "A common scenario might involve the author of the work having created a fake website designed to look like a legitimate website, and a financial institution (Computer Hacking Forensic Investigator, 2009).

2.5. Identity Theft in Kosovo Banks - Electronic Communication

Identity theft is the process of getting personal information from a person or organization pretending to be someone else. This is often done to obtain credit on behalf of the victim, putting this in financial liabilities. So, it's about stealing a person's identity and then that identity is used to commit fraud with the victim's personal information, such as: insurance numbers, bank accounts, and credit card numbers. Identity thieves provide the names, addresses, dates of birth of the victims and can apply for loans on their behalf (Easttom, 2011).

It is important to consider the means by which identity theft is committed. The most important action for perpetrators is access to personal information so that it can be used in identity theft. There are four main ways in which individuals access personal information: phishing, or spyware hacking, unauthorized data access, and deletion of information. Another form is credit card fraud. Attackers illegally use someone else's credit card to buy other goods and services online. Also, by using different techniques, they can steal personal data in a user's online transactions or simply through social engineering techniques.

According to the Kosovo Banking Association, computer system fraud can cause significant damage, so the Kosovo Banking Association presents some recommendations to businesses in order to better protect themselves from cyber-attacks: “To provide computer systems with antivirus, to have installed Antivirus and keep it updated regularly. Also, other applications such as browsers (Explorer, Firefox, Chrome) keep up to date, not send personal information, in particular username, password and credit card information via email, social media messages ('Face book 'etc.).

3. Recommendations and Conclusions

This paper deals with various cryptographic algorithms and techniques that provide data security in various aspects of functional operation. Initially their operational structure is given by examining the relevant features that are the basis for a robust cryptographic scheme.

Certain algorithms have different performances depending on how they are applied and where they are applied but we also know that a symmetric algorithm is faster than an asymmetric algorithm. The level of security is subjective: an algorithm may be very safe but not efficient, or it may be less secure but at the same time more efficient. It depends on what we ask for and can spend. In this paper, the sites of application of cryptography are reviewed. Much of the cryptographic attack depends precisely on the computer capabilities of computer systems.

A certain number of attacks aim to find deficiencies in the operational structure of a cryptographic algorithm while another part points out weak points in its implementation. Powerful encryption algorithms such as AES, RSA and ECDSA, although considered perfect in structure, are somewhat fragile in implementation (it is possible to obtain the key used in encryption).

The use of cryptographic algorithms in everyday applications drives us to recognize and focus on today's encryption techniques and even identify potential cases of data protection and communications breaches. For this reason we have attempted to provide a broad overview of the use of algorithms by examining the possibilities of application in different countries. In this way we have tried to identify points and issues that are critical to data protection.

References

1. Zenullahu,Hamit “Bazat e Kriptografisë” Prishtinë, 2011–243f. ISBN 978-9952-585-99-6
2. Dawid Kahn, The Codebreakers, Scribner, New York, Ny 10010;
3. Joachim Beckt, Blitz &Anker Band II , ISBN 3-8334-2997-6;
4. Zenullahu,Hamit “Bazat e Kriptografisë” Prishtinë, 2011–243f. :ISBN 978-9952-585-99-6
5. Simon Singh, Geheime Botschaften, KmbH & CO. KG, Munchen, 2001;
6. “A survey of information authentication”, G. J. Simmons, editor, Contemporary Cryptology: The science of Information Integrity, 379-419, IEEE Press, 1992.
7. Easttom, C. (2011:5), Computer crime, investigation, and the law. Cengage Learning, USA.
8. Computer Hacking Forensic Investigator, 2009.
9. Easttom, C. (2011:6), Computer crime, investigation, and the law. Cengage Learning, USA.
10. https://www.gazetaexpress.com/lajme-krimet-kibernetike-ne-rritje-ne-kosove-qasur. date 06.09.2019
11. Easttom, C. (2011:5), Computer crime, investigation, and the law. Cengage Learning, USA.