RF Signals Encryption with AES in WDID

Serhii Toliupa, Volodymyr Nakonechnyi, Maxym Kotov and Valeriia Solodovnyk

Taras Shevchenko National University of Kyiv, Bohdana Havrylyshyna 24, Kyiv, 04116, Ukraine

Abstract

This article reflects the usage of symmetric encryption algorithms in remote input devices. Information on currently available encryption algorithms and the use of hash functions is provided. The difference between encryption methods with one and two keys is highlighted. AES algorithm, its data encryption scheme, and rounds are considered in detail. The description of the presented algorithm is accompanied by an example that explains the specifics of its use. A mathematical model and an example of a block encryption algorithm are illustrated. The work principles of wireless devices are given. Vulnerabilities related to wireless devices are considered and solutions are proposed.

Keywords [1]

cryptography, encryption, block encryption, signal encryption, symmetric encryption, wireless data input devices

1. Introduction

Nowadays, there are many computer systems which purpose is to improve and facilitate people's lives. Considering that the number of researchers that are interested in the field of information processing is increasing, the development of computer systems is rapidly gaining momentum. Due to the rapid development of information systems, new threats are emerging, such as breaches of confidentiality, integrity, and availability of information. To prevent possible data loss, modern information security systems are being constantly updated and improved. Since it is impossible to create a fully secure system, there is always the possibility of data theft. Therefore, there is a problem with the protection of information and telecommunications systems, which is becoming increasingly important. Given that no protection can be perfect, a method has been developed to significantly reduce data breaches. For clarity, we can give examples such as steganography and cryptography. The purpose of steganography is to conceal the information storage, whereas for cryptography - it is necessary to perform the concealment of transmitted information content. Using modern cryptographic algorithms to encrypt information, it is possible to keep it confidential, even if unauthorized access takes place. Currently, cryptosystems are used to protect information and telecommunications systems and other technologies, in particular, to protect critical information of a country, individuals, businesses, or other important data, such as trade secrets or intelligence. Therefore, the reliability of cryptosystems depends on the fulfillment of such requirements as secret key storage, generation of pseudo-random numbers, the chosen encryption algorithm, etc [1-5].

A significant contribution to the development of cryptography and cybersecurity is made by the works of such authors as Kuznetsov O.O., Gorbenko I.D., Kavalchuk L.V., Dan Bone, Victor Shup, S. Tolyupa, L. Slipachuk, V. Nakonechny, M.M. Brailovsky, William Stollings [1-6]. Symmetrical encryption is described in the scientific works of Joseph Sterling Gra, Nigel Smart, Christoph Pair, Jan Pelsl [7-11]. The use and operation of the AES cipher are considered in the works of Joan Damen, Vincent Ridgman [12, 13]. The results of studies of block encryption algorithms contained in the works of A.V. Yakovlev, A.A. Bezrogov and V.V. Rodina, V.N. Samka, Roberto Avanzi, Bruce Schneier, Lars R. KnudsenMatthew J. B. Robshaw [14-21]. Studies in the field of radio signals by the following authors were also considered: V. Saiko, S. Tolyupa, V. Nakonechny, and Dakov Serhiy [22].

IT&I-2020 Information Technology and Interactions, December 02–03, 2020, KNU Taras Shevchenko, Kyiv, Ukraine

EMAIL: tolupa@i.ua (A. 1); nvc2006@i.ua (A. 2); shunki2001@ukr.net (A. 3), valeriamin6@gmail.com (A. 4)
ORCID: 0000-0002-1919-9174 (A. 1); 0000-0002-0247-5400 (A. 2)

Recent events in the world had confirmed the importance of counteracting violators and attempts to conduct information warfare which purpose is to inflict losses. Sufficiently detailed analysis also confirmed that along with other methods and mechanisms of information protection, those based on cryptographic transformations of information are important. Indeed, with the right choice and application, in accordance with the requirements of cryptographic transformations, a high level of security could be achieved and, accordingly, the main services - confidentiality, integrity, protection against unauthorized access, accessibility, irrefutability, etc. In cryptographic protection of information, cryptographic stability, integrity, speed of cryptographic transformations, and requirements set by applications are put forward and must be ensured.

It is clear that cryptographic stability is an unconditional requirement, but along with it, speed is also an unconditional requirement - it is needed to protect channels at speeds ranging from hundreds of megabits to tens of gigabits per second, performing real-time operations. This requirement could be met by applying cryptographic transformations such as block symmetric cipher.

However, the problem of information protection during its transmission in wireless data input devices (WDID) is still significant. This article focuses on improving the security of wireless data input devices using cryptographic systems.

2. Statement of the main material

Cryptography is the science that creates strategies for utilizing complex mathematical transformations to transmit data through conveyance channels in a frame that no one but authorized persons can get. An encryption process is a key object in the field of cryptographic research, it is the method of changing the frame of data which is transmitted through open transmission channels [1, 2].

An encryption transformation may be a set of converse numerical capacities that change plain text into an encrypted state. There are 3 fundamental sorts of information encryption [1]: encryption utilizing two keys; encryption with a single key; keyless encryption.

The fundamental distinction between keyless, one-key, two-key transformations is within the preparation of plain content encryption. Keyless systems do not utilize keys within the handle of cryptographic change of plain text. Examples of such transformations are hash functions and pseudo-random number generators [5]. Hash is a function that changes an input of self-assertive size information into a fixed-length bit string and is executed employing a particular calculation.

Usually hash capacities are utilized for construction of special identifiers, calculation of checksums for errors detection that happen amid transmission of data, seeking for copies in arrangement of information sets, construction of acquainted arrays, storing of passwords in security frameworks within the frame of a hash code [6, 7]. One-key systems utilize a key to encrypt and decrypt information within the process of cryptographic change of data. The encryption key may comprise numbers, words, or symbols. Since everyone with access to a key can decrypt the data, such a key should be kept in secret, and be known exclusively for the sender and recipient, to guarantee encryption unwavering quality [5]. The utilization of the one-key system is shown in Figure 1.

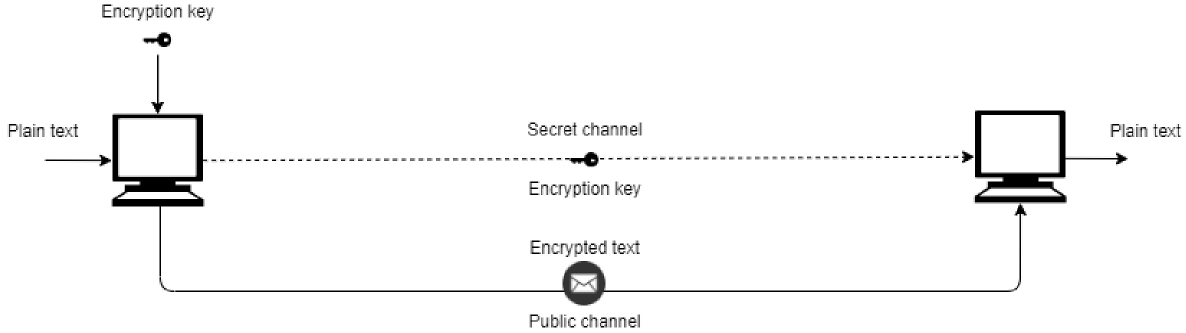

Figure 1: Symmetric encryption system key exchange scheme

As famous over, symmetric encryption utilizes one private key to transform the plain text. If the encryption algorithm is crypto-resistant sufficiently, the only way for an assailant to decrypt data is to get a key. Two-key encryption is an information encryption method that uses two encryption keys: public and private. The main benefit of asymmetric encryption is that it is dispensed with the requirement of the key transmission through the protected secret channel [5].

In common, general steps of message exchange are [5]:

1. first user creates two keys - public and private;
2. then the first user passes the public key to the individual who sends the message, and leaves the private key for himself;
3. after receiving the public key, second user encrypts the data utilizing that key and sends the encrypted text.

The only person that can decrypt this message is a private key proprietor. It isn't conceivable to decrypt this message with the public key. In this manner, it isn't required to utilize classified communication channels to transmit the key. The scheme of the asymmetric system usage is shown in Figure 2.

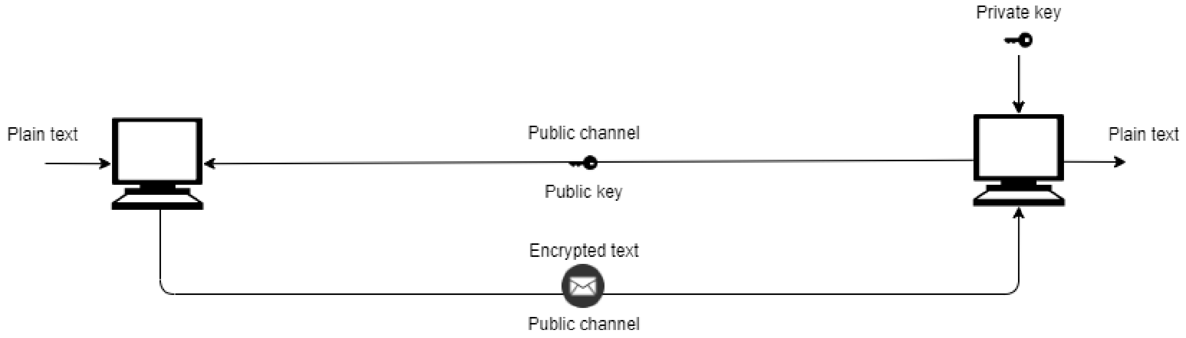

Figure 2: Asymmetric encryption system key exchange scheme

The quality of the encryption is measured by the time that it takes to decrypt the content with brute force which is checking all conceivable key combinations. An algorithm is unsafe if half of all conceivable key combinations may be checked in a brief time. Modern computers will be able to get a 128-bit key in billions of years, and in turn, 256-bit keys are considered secure and hypothetically able to resist the onslaught of quantum computers [8-11].

Cryptographic information protection systems that are practically used, usually have such a length of the message protected by the symmetrical block encryption that significantly exceeds the length of the encryption key. In this case, the criterion of unconditional stability of the used cipher is not met, and in such conditions, it is advisable to introduce a polynomial criterion, which implies the existence of restrictions on the computing resources of the attacker and the time during which the cipher remains stable. The polynomial criterion leads to a practical criterion of stability - the impossibility of implementing an attack on the cipher in a modern computer base for a long time.

Additionally, given the possibility of improving cryptanalytic methods, the criterion of "margin of resistance" to analytical attacks is introduced - the complexity of the attack on the whole algorithm should be much higher than the complexity of force attacks. Typically, this criterion considers a version of a symmetric block encryption algorithm with a reduced number of cycles that is vulnerable to cryptographic analysis. The difference in the number of cycles determines the margin of stability of the algorithm for a particular cryptanalytical attack.

To assess the cryptographic stability of the overall structure of the cipher, it is advisable to introduce another criterion that considers the possibility of excluding any operations or replacing them with less complex operations (for example, on some input sets the addition operation modulo 2^{32} is close or equivalent to the addition operation modulo 2). In this case, the full-cycle version of the simplified cipher must remain resistant to analytical attacks.

It should also be borne in mind that most modern analytical attacks, primarily such as differential and linear cryptanalysis, are statistical. When performing cryptanalysis to obtain a key, a large amount of encryption is performed, and on the basis of ciphertexts, subkey options are formed.

When processing a large enough sample of ciphertexts generated on one key, the correct value of key bits is more common than other options. Obviously, the probability of finding the correct pair (which suggests the correct value of the key) depends on the statistical properties of the cipher, and to increase the complexity of cryptanalysis, the properties of the cryptogram should be close to the properties of a random sequence. Therefore, a necessary (but not sufficient) condition for the stability of the cipher to analytical attacks is to ensure good statistical properties of the original sequence (ciphertexts). To protect the cipher from algebraic attacks, it is necessary that there is no way to practically build a system of equations that link plaintext, cryptogram, and encryption key, or there is no way to solve such systems in polynomial time.

While constructing cryptographic protection, it is necessary to consider the possibility of organizing attacks on the implementation (change in temperature of the electronic device, input voltage, the appearance of ionizing radiation, measurement of currents consumed, execution time, etc.). Such attacks can be effective against all cryptographic algorithms, and protection against such attacks requires engineering solutions when designing cryptographic information security tools.

There are two sorts of symmetric encryption [11]:

1. block encryption;
2. stream encryption.

The names of these types were inferred from the strategy of input content processing. Block encryption process operates with settled pieces such as 128 bits by applying encryption transformations and 128, 192, or 256-bit key.

The block cipher scheme is shown on Figure 3.

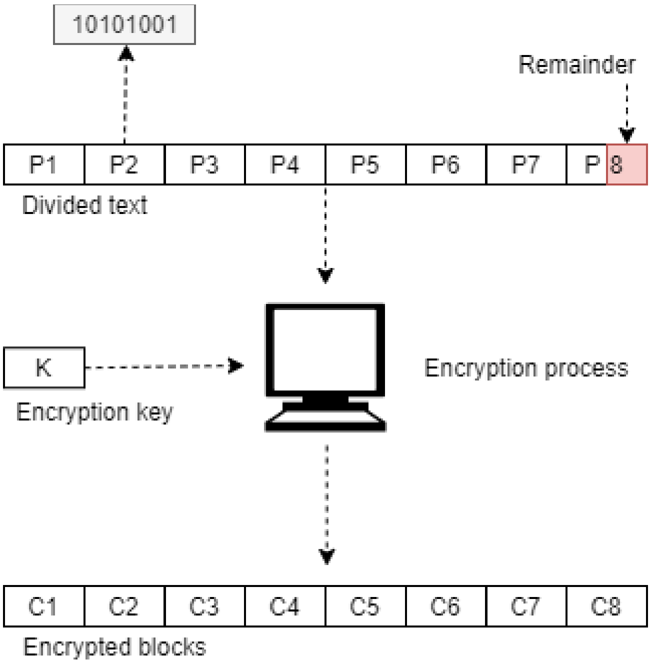

Figure 3: Block cipher encryption process scheme

Stream ciphers, in turn, work with each bit of the input content and yield bit by bit of the encrypted text. Stream ciphers convert plaintext to ciphertext, one bit per operation. The keystream generator produces a bitstream. The processes of encryption and decryption involve XOR operations between bits of plain text bitstream and keystream.

An example of a symmetric block encryption algorithm is the AES competition finalist, the American encryption standard - Rijndael [12]. AES 128 was chosen for analysis. In this form of the algorithm, the cipher key comprises 128 bits isolated by 16 bytes that are arranged into the *InputKey* matrix. The *InputKey* comprises 4 columns. Utilizing those columns an arrangement of 44 words (w0 - w43) where each word comprises 32 bits is shaped. Thus, these words become the round keys. The AES scheme is shown in Figure 4.

Considering the diagram in Figure 4, encryption and decryption of messages are performed over ten rounds where each round has an operation of key addition. As an example, suppose we have 128 bits of input message *A* and 128 bits of round key *K*, at the beginning operation *AddRoundKey* is performed, which is *XOR* operation of the input text with the key: *B* = *A XOR K*, where *B* is 128-bit text after the operation *AddRoundKey*. Each round of AES encryption and decryption consists of four transformations [12].

The following transformations are performed for the encryption round:

1. *SubBytes* - byte substitution in S-BOX, with fixed replacement table. *SubBytes* – is a transformation that performs a nonlinear replacement of each byte of the *State* matrix. Using *S-BOX*, byte *I* is converted at the input to byte *S* = *SubBytes (I)*, in the field *GF (2)*.
2. *ShiftRows* - byte rows offset of the *State* matrix. During this operation, the first row of the matrix remains unchanged, the bytes of the second line are shifted to the left by one position, the elements of the third line are transferred to the left by 2 positions, the bytes of the fourth line are

shifted to the left by three positions, if further transfer to the left is not possible, the countdown continues from the end of the line.

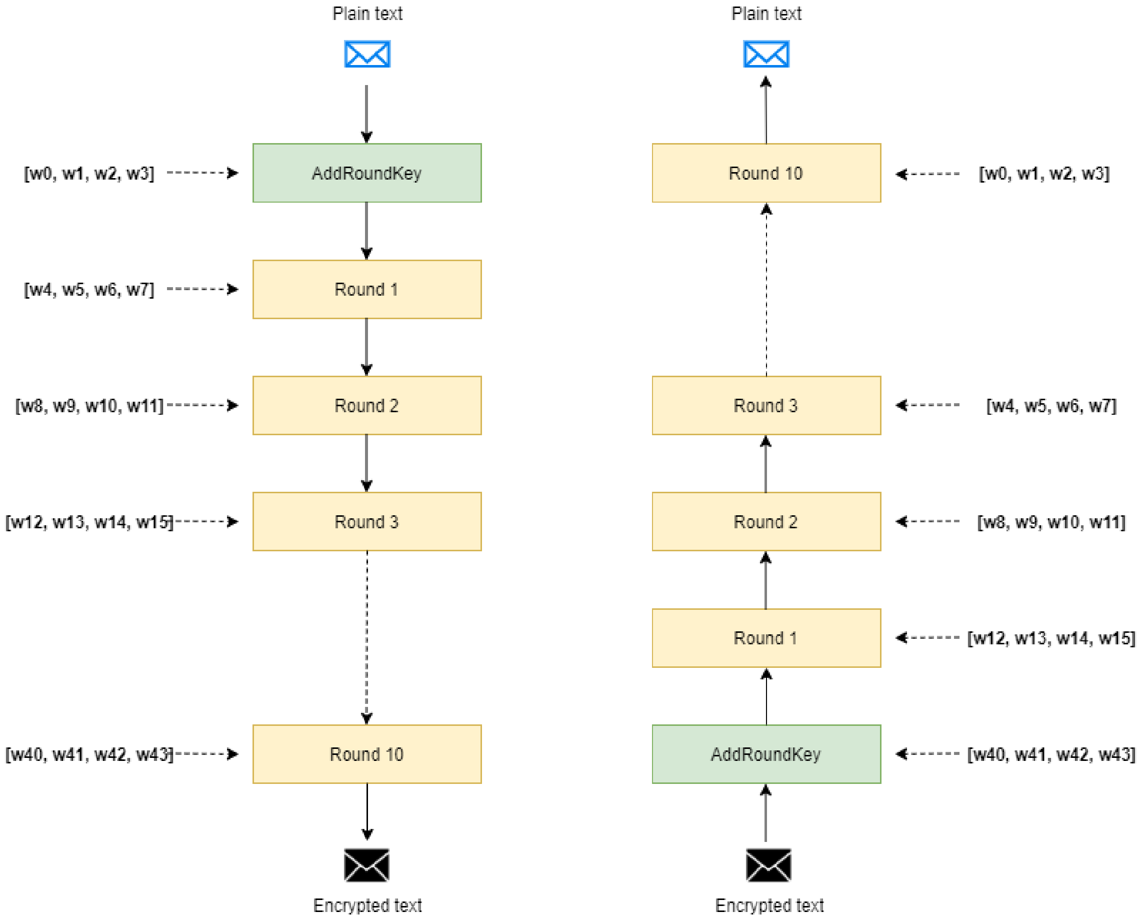

Figure 4: AES encryption process scheme

3. *MixColomns* - performs byte mixing in the columns of the matrix. Each column of the *State* matrix is used as a polynomial over the field *GF* (2^8) and multiplied by a fixed polynomial *c (x)*.
4. *AddRoundKey* - an operation that performs a byte summation modulo 2 of each element of the State matrix, with each corresponding element of the round key matrix.

The following transformations are performed for the decryption round:

1. *InvShiftRows*;
2. *InvSubBytes*;
3. *AddRoundKey*;
4. *InvMixColomns*.

The last round of encryption differs from the others in that it does not activate the MixColomns conversion [13]. Figure 5 presents a scheme of the transformations in each encryption and decryption rounds. It is important to estimate the cryptographic stability of an algorithm according to the Kerckhoffs theorem, considering that the attacker knows all the procedures for transforming the input text that the algorithm performs. This means that only encryption key remains in secret [14, 15].

The time required to check all possible key combinations from the assailant's side dictates whether it is rational to conduct a brute force, as data encryption with a longer key is far more reliable.

For illustration, let's take a key with a length of 4 bits, utilizing the essential laws of combinatorics it is conceivable to calculate all possible combinations: $S = 2 * 2 * 2 * 2 = 16$. In this way, the number of possible alternatives is $S = 16$. Suppose we have 100 machines that check 10,000,000 combinations of encryption key per second, the algorithm is considered to be unsafe if half of the variants could be checked in a short period of time. With those parameters, Table 1 was made. Considering the results of measurements in Table 1, it can be inferred that the 128-bit length key encrypts the data securely. The 256-bit key is theoretically resistant to the brute-force attack of quantum computers.

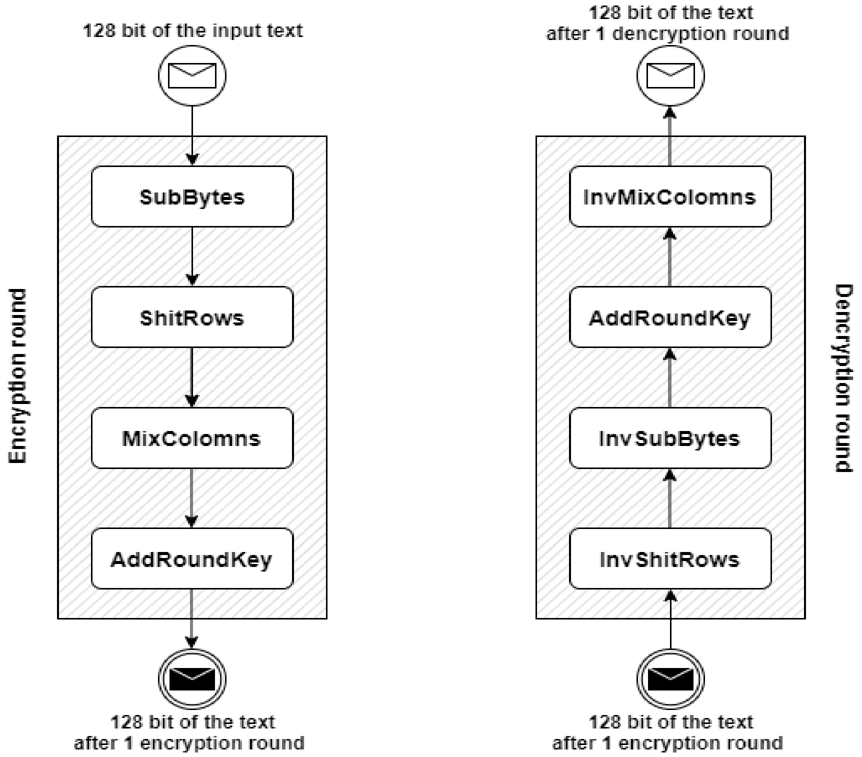

Figure 5: AES encryption and decryption rounds

Table 1
Key Combinations

Key size	Combinations	Time
1	2	2 * 10^(-10) sec
2	4	4 * 10^(-10) sec
4	16	1.6 * 10^(-9) sec
8	256	2.56 * 10^(-8) sec
16	65 536	6.5536 * 10^(-6) sec
32	4 294 967 296	0.42 sec
56 (DES)	7.20575940 * 10^16	83.39 days
64	1.84467441 * 10^19	58.49 years
128 (AES)	3.40282367 * 10^38	1.08 * 10^21 days
192 (AES)	6.27710174 * 10^57	1.99 * 10^40 days
256 (AES)	1.15792089 * 10^77	3.67 * 10^59 days

3. Block encryption mathematical basics

Block encryption is an encryption scheme that uses transformations at every clock of its operation, depending on the algorithm chosen at the start of its operation. The block cipher algorithm is considered to be a substitution cipher, but its main characteristic is that there is a large alphabet in this cipher. The series of binary numbers 0 and 1, i.e. binary data of a certain size [16-21]. Let's take a block of size *N* (sequences 0 and 1) as an example of how this method works: *p = (p0, p1, p2,..., pN-1) Î Z2, N*, where *p Î Z2, N* is a vector represented by fixed lengths 0 and 1. Then we get the number's binary presentation by substituting the details in the formula:

$$\left|\left|p\right|\right| = \sum_{i=0}^{N-1} 2^{N-i-1} p_i. \tag{1}$$

Then it becomes obvious that the reliability of the cipher depends on the size of the replacement tables, which cannot be physically represented due to the size of their volumes. Let's create the following table. For example, let's take N = 5, then table will look like the following one:

Table 2
Replacement table

(0,0,0,0,0)→0	(0,0,0,0,1)→1	(0,0,0,1,0)→2	(0,0,0,1,1)→3
(0,0,1,0,0)→4	(0,0,1,0,1)→5	(0,0,1,1,0)→6	(0,0,1,1,1)→7
(0,1,0,0,0)→8	(0,1,0,0,1)→9	(0,1,0,1,0)→10	(0,1,0,1,1)→11
(0,1,1,0,0)→12	(0,1,1,0,1)→13	(0,1,1,1,0)→14	(0,1,1,1,1)→15
(1,0,0,0,0)→16	(1,0,0,0,1)→17	(1,0,0,1,0)→18	(1,0,0,1,1)→19
(1,0,1,0,0)→20	(1,0,1,0,1)→21	(1,0,1,1,0)→22	(1,0,1,1,1)→23
(1,1,0,0,0)→24	(1,1,0,0,1)→25	(1,1,0,1,0)→26	(1,1,0,1,1)→27
(1,1,1,0,0)→28	(1,1,1,0,1)→29	(1,1,1,1,0)→30	(1,1,1,1,1)→31

The block cipher is indicated as follows: $\pi \in SYM(Z_{2,N})$; $\pi{:}p \rightarrow q = \pi\ (p)$, where $p = (p0, p1, p2,..., pN\text{-}1)$, $q = (q0, q1, q2,..., qN\text{-}1)$. As described above, a block cipher is a special case of a broad alphabet replacement, but due to its common use today, this type of cipher is considered separately, since it is much simpler and more convenient to explain it with algorithms.

Many cryptosystems are implemented using block ciphers, since constructing a chain of bytes pre-encrypted by this algorithm is the process by which they are used. This allows the encryption of information which batch volume is unlimited [16].

The source text is encrypted with the replacement π, which is selected from the complete symmetric group. Then, even with this cipher knowledge, an attacker who attempts to conduct an attack and attempts to match the encrypted and source text $pi \leftrightarrow qi,\ 0 \leq i \leq m$, cannot locate the source text that has the following correspondence: $q \notin \{qi\}$ [20]. Then it would be correct to say that the block cipher is a special case of replacement by a mono-alphabet, and its alphabet can be written as follows:

$$Z_2{}^N = Z_{2,N}. \qquad (2)$$

P[K]- this is a subset of the *SYM(Z2,N)* symmetric group and the cipher key block scheme. It is indexed by the $k \in K$ parameter, where the value is *k* and the key space is *K*.

The expression *P[K]* is a mathematical notation:

$$P[K] = \{\pi\{k\}\colon k \in K\} \qquad (3)$$

As for *N = 5*, we use the same table construction theory, and we will consider other instances. Let *N = 64* and then each *SYM(Z2,N)* element can potentially be regarded as a substitute, so that *K = SYM(Z2,N)*.

It is accompanied by the following statements:

- 2^{64} are 64 digits, but the intruder is unable to hold a directory with a size of approximately $2^{64} \approx 1.8 \approx 1019$ lines;
- the attempt to obtain the key is equal to (2^{64}).

The integrity of block cipher systems is demonstrated by the alphabet $Z_{2,64}$, the key space $K = SYM(Z_{2,N})$ and, most significantly, the size of the 64-bit block character input directory, given that the number of keys is 2^{64}, or that it is beyond its capabilities, an attempt to acquire a key by an attacker is impossible.

At the same time, the attacker faces the problem of insufficient resources, which limits its capabilities, thereby ensuring the proper functioning of the system. This is similar to the situation when an attacker tries to perform cryptanalysis of text data.

It is unfortunate to realize that both the attacker and the developer have the same problem. The reasons for this problem are explained by the following factors [16]:

- the developer himself does not have the opportunity to build a method in which 2^{64} substitute *SYM* $(Z_{2,64})$ could be implemented;
- the intruder is unable to read any of this group's keys.

For a block cipher, it is possible to formulate the following specifications [16]:

- *N*-should be at least 64 and more than 64 ideally. This is important when generating a directory for complications;
- the space of the keys should be as wide as possible in order to exclude the risk of choosing them;
- $\pi\ \{k, p\}\colon p \rightarrow y = \pi\ \{k, p\}$ - the relation between the source and the cyphertext must be complicated in such a way that statistical or analytical analysis methods can not be used on the basis of the correspondence between the source text or the key.

Therefore, it follows that the crypto algorithm used to encrypt the data should be perfectly reliable, and that could be done if the output is readable only in case when key variants are known. Turning to the theory of probability, we understand that after searching for half of all keys, the necessary key will be found with a probability of 0.5. It follows that the stability of the block cipher depends entirely on the length of the key. This causes the stability of the cipher that increases exponentially at the same time with the length of the key.

And even though we could presume that the key sorting would be carried out in a special multiprocessor device, it would take too long to split a 128-bit key. Then we understand that it is irrational to decrypt by frontal assault. All this, of course, refers only to perfect ciphers, the implementation of which, due to different physical factors, is impossible [18].

4. Remote input devices signal encryption

There are numerous wireless input devices in access nowadays. As the devices of wireless information input we consider - the gadget of remote transmission of the entered information to the computer (wireless data input device WDID). Examples of such gadgets are remote consoles or mice, remote headsets, touch input gadgets, etc.

WDID gadgets transmit data through radio waves with a frequency from 27 MHz to 2.4 GHz. WDIDs perform their work with a transmitter and a collector [23, 24]. The fundamental issue with gadgets that transmit data at 2.4 GHz is that there's no uniform standard for transmitted data protection. In case of connection of the devices such as wireless laptop mouse without device authentication, the possibility of cursor manage interception takes place. A few models of wireless keyboards use signal encryption but, in most cases, the safety of wireless devices isn't always getting a lot of interest.

So, for example, computer mouse signal encryption is not commonly used, and keyboard signal encryption is also not performed. This permits attackers to intercept signals and get personal records. Regardless of keyboard encryption, the threat remains feasible. An example of a records acquisition technique is Mousejack. Even such tremendous businesses as Dell, Logitech, Microsoft, HP, Amazon, Gigabyte, and Lenovo will now not be able to face up to this assault [25]. This assault may be accomplished at distances of up to one hundred meters, and all that is needed for an attacker is a USB dongle [25-28].

The essence of this attack is in the following stages. A wireless keyboard and a wireless mouse use USB-dongle for signal transmission. a few models of keyboards encrypt those signals, but the majority of mice do not. In the case of keyboards, this works as follows [24]: only USB dongle has the encryption key, which makes it the only item that has the potential to decrypt a signal, an attacker, even though he intercepts that signal, will no longer be able to decrypt it. But as it was stated most of the mouses are not encrypting their broadcast and so the attacker is able to receive unencrypted packets. Figure 7 shows the 1-3 phases of this attack.

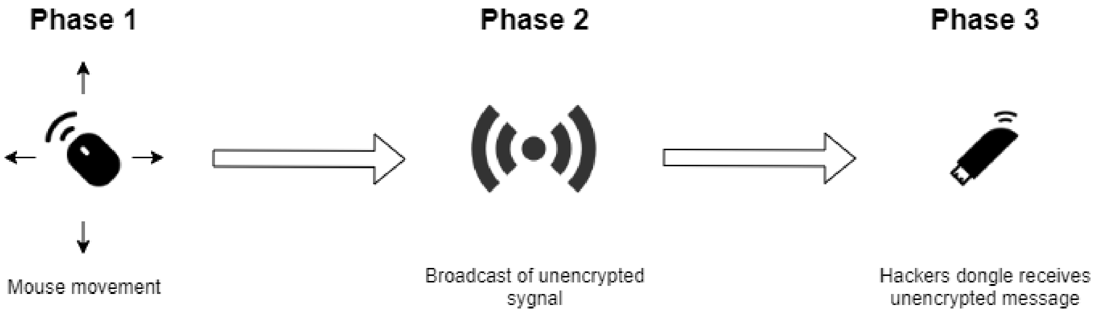
Phase 1
Phase 2
Phase 3
Mouse movement
Broadcast of unencrypted sygnal
Hackers dongle receives unencrypted message

Figure 6: 1-3 phases of MouseJack

The following happens during the first three steps: the user determines the shift (x, y) of the mouse location coordinates, and the transmitter in the mouse transmits the radio signals without encryption to the USB-dongle. At the same time, hackers intercept unencrypted signals using their own personalized USB dongle.

Figure 8 shows the 4-6 phases of the attack on MouseJack.

The attacker sends a series of characters to the user's machine during Step 7-9. If all the stages shown above have succeeded, the hacker has full access to the computer of the victim [25]. The vulnerability can be used on all operating systems since this vulnerability does not apply to operating system vulnerabilities. An intruder can install malware, access computer data, delete data, compromise its integrity or availability using this vulnerability.

The use of reliable encryption algorithms, such as the AES algorithm discussed above, is therefore a way to protect against this weakness in the signal transmission mechanism of WDID. Simple identification of devices trying to send USB dongle packets is required to be established. The downside of using encryption is an expansion in response time, that is, the pacing.

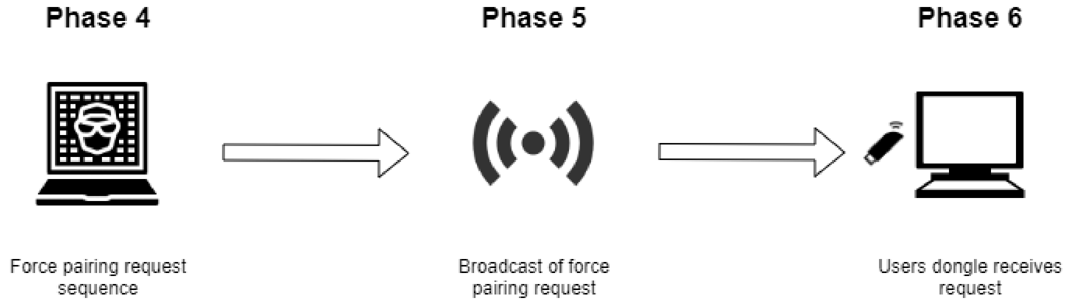
Phase 4
Phase 5
Phase 6
Force pairing request sequence
Broadcast of force pairing request
Users dongle receives request

Figure 7: 4-6 phases of MouseJack

The attacker sends a sequence of requests to connect to the USB dongle during 4-6 stages, then the USB dongle receives the sequence of these requests and connects to the computer of the user [25].

Figure 9 demonstrates the 7-9 stages of the assault on MouseJack.

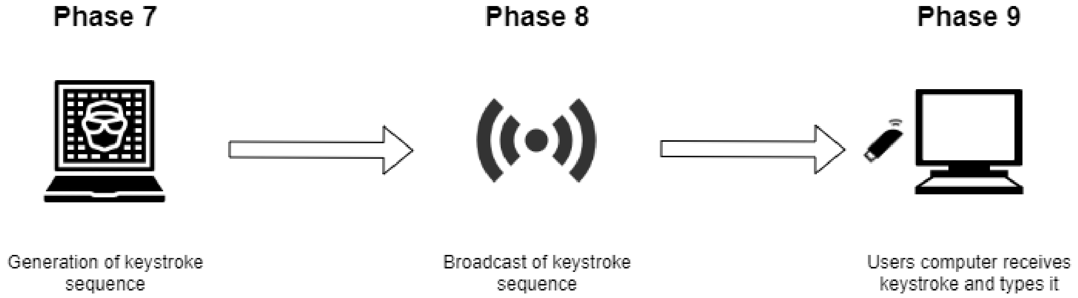
Phase 7
Phase 8
Phase 9
Generation of keystroke sequence
Broadcast of keystroke sequence
Users computer receives keystroke and types it

Figure 8: 7-9 phases of MouseJack

5. Conclusions

Today, for information and cybersecurity practitioners, data protection is a top priority. Among the enormous variety of attacks and attempts to steal data, development of the successful defenses is becoming increasingly difficult for professionals.

Every action has its implications and, thus, emerging technology, which on the one hand, makes our lives simpler and, on the other hand, creates new challenges to the security, integrity, and availability of information within the system. This article is intended to cover methods of defense against the capture of information while entering it using wireless data input devices. Therefore, the article provides a general overview of encryption algorithms as one of the forms of information security. There is a list of the most popular forms of encryption and information about them. Examples of how such approaches are implemented during data protection are also added. As the most prevalent algorithm to date, this article highlights symmetric encryption algorithms, namely the AES algorithm. Its benefits, drawbacks, and variety are emphasized. Block encryption algorithms are considered and their mathematical model is constructed. It should be kept in mind that there are some benefits to the usage of the algorithm, namely reliability. In order to encrypt radio frequency (RF) signals due to vulnerabilities that may occur because of unencrypted RF signal transmission, it is proposed to use symmetric cryptographic algorithms in wireless data input devices.

6. References

[1]. Dan Boneh, Victor Shoup, A Graduate Course in Applied Cryptography, version 0.4, Stanford University, Standford, September 2017.

[2]. S. Toliupa, L Slipachuk,. V. Nakonechnyi. The Process of the Critical In-frastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine, 3rd International Conference on Advanced Information and Communications Technologies, Proceedings: AICT 2019, Lviv, 2019.

[3]. S.V Toliupa, V.S. Nakonechny., N.N. Brailovskyi, Building Cyber-Security Systems of Information Networks Based on Intellectual Technologies, p. 620, Scientific & practical cyber security journal (SPCSJ) №1, Kharkiv, SMIT Company, 2017.

[4]. William Stallings, Cryptography and Network Security Principles and Practices, 4th ed., Prentice Hall, New Jersey, 2005.

[5]. 60 cryptoalgorithms. Part one: Keyless CAs, URL: https://www.pvsm.ru/algoritmy/225093#begin

[6]. Bruce Schneier. Applied cryptography. Protocols, algorithms, source texts in the C language, 20th ed., New Jersey, Wiley, 1995.

[7]. Joseph Sterling Grah, Hash Functions In Cryptography, The University of Bergen, Bergen, Norway, 2008.

[8]. What Is Symmetric Key Cryptography?, URL: https://www.binance.vision/security/what-is-symmetric-key-cryptography

[9]. Nigel Smart, Cryptography: An Introduction, 3rd edition, Mcgraw-Hill College, New York City, NY, 2004.

[10]. Symmetric-key algorithm, URL: https://en.wikipedia.org/wiki/Symmetric-key_algorithm

[11]. Christof Paar, Jan Pelzl, Understanding Cryptography, Springer-Verlag Berlin Heidelberg, Berlin, 2010.

[12]. Joan Daemen, Vincent Rijmen, AES Proposal: Rijndael, Belgium, 1999.

[13]. Joan Daemen, Vincent Rijmen, The Design of Rijndael, Springer-Verlag, Belgium, 2001.

[14]. C. E. Shannon, Communication Theory of Secrecy Systems, volume 28, Nokia Bell Labs, New York, NY, 1949. doi: 10.1002/j.1538-7305.1949.tb00928.x

[15]. Kerkhoffs principle, URL: https://dic.academic.ru/dic.nsf/ruwiki/12112

[16]. A.V. Yakovlev, A.A. Bezbogov, V.V. Rodin, V.N. Shamkin, Cryptographic information protection, Tambov State Technical University Publishing House, 2006.

[17]. Block codes, URL: https://studref.com/403682/informatika/blochnye_shifry

[18]. Roberto Avanzi, A Salad of Block Ciphers, Munich, 2017.

[19]. Bruce Schneier, A self-study course in block-cipher cryptanalysis, Cryptologia, volume 24, 2000. URL: https://doi.org/10.1080/0161-110091888754

[20]. Replacement codes, URL: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema4

[21]. Lars R. KnudsenMatthew J.B. Robshaw, The Block Cipher Companion, Springer-Verlag Berlin Heidelberg, 2011.

[22]. V. Saiko, S. Toliupa, V. Nakonechnyi, and Dakov Serhii, The method for re-ducing probability of incorrect data re-ception in radio channels of terahertz frequency range, 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018. S 11. № 215. # 174.

[23]. How Does a Wireless Keyboard and Mouse Work?, URL: https://techspirited.com/how-does-wireless-keyboard-mouse-work

[24]. How does a wireless keyboard for a computer work?, URL: https://compfonyk.com/kak-rabotaet-besprovodnaya-klaviatura-dlya-kompyutera/

[25]. Mousejack Attack: Critical Vulnerability Found in Wireless Mice and Keyboards, URL: https://habr.com/ru/post/390767/

[26]. Interception of data from wireless keyboards is now available to everyone, URL: https://www.securitylab.ru/news/381480.php

[27]. 'MouseJack' Attack Bites Non-Bluetooth Wireless Mice, URL: https://www.darkreading.com/endpoint/mousejack-attack-bites-non-bluetooth-wireless-mice/d/d-id/1324404

[28]. Sklyarov D. V. Hardware security keys, Art of protection and information hacking, SPb, BHV-Petersburg, 2004.