http://dergipark.ulakbim.gov.tr/tujes
*Trakya University Journal of Engineering Sciences, 17(1): 1-11, 2016*
*ISSN 2147–0308*
**Araştırma Makalesi / Research Article**

# COMPARISON OF ENCRYPTION ALGORITHMS STRENGTH USED IN 3G MOBILE COMMUNICATION

Fatma AKGÜN[1], Ercan BULUŞ[2]

[1] Department of Computer Education and Instructional Technologies, Trakya University, Edirne-TURKEY
e-mail: fatmaa@trakya.edu.tr
[2] Department of Computer Engineering, Namık Kemal University, Çorlu/Tekirdağ-TURKEY
e-mail: ercanbulus@nku.edu.tr

**Abstract:** In this study, the strength of data encryption algorithms used in UMTS and CDMA2000 systems which are 3G mobile communication technologies were analyzed. At the beginning of the study, software applications were developed for KASUMI encryption algorithm which is used within UMTS system and AES encryption algorithm which is used within CDMA2000 system. Both key generation algorithms are applied to the same key values to create new key values which are used for data encryption. These new key values are tested by using test package of NIST to in order to check whether these key values are generated randomly or not. One of the key value which has high randomness is used as encryption key As a result, it was observed that AES algorithm is more successful than KASUMI algorithm in generating key values. Additionally, a key value, which has high randomization, was chosen and this key value was applied on encryption algorithm with plain text statement and as a result application of encrypted text on NIST test, it was observed that both KASUMI and AES block encryption algorithms have equally power in 3G mobile technology.
***** This paper is based on a Ph.D study titled "The Structure of Mobile Communication Technologies and Analysis of the Reliability of Data Encryption Algorithms Used in These Technologies"

**Keywords:** Security, Mobile communication, KASUMI, AES, NIST tests

## 3G Mobil Haberleşme İçerisinde Kullanılan Şifreleme Algoritmalarının Gücünün Karşılaştırılması

**Özet:** Bu çalışmanın amacı 3G mobil iletişim teknolojilerinden CDMA2000 ve UMTS sistemlerinde yer alan veri şifreleme algoritmalarının gücünün karşılaştırılmalı analizidir. Öncelikle UMTS teknolojisi içerisinde yer alan KASUMI şifreleme algoritması ve CDMA2000 teknolojisi içerisinde yer alan AES şifreleme algoritmaları için yazılım geliştirilmiştir. Yeni şifreleme anahtarları elde etmek için her iki anahtar üretme algoritmasına aynı anahtar değerler uygulanmış ve elde edilen yeni anahtar değerler rassallıkları test edilmek üzere NIST testlerinden geçirilmiştir. Rassalığı yüksek olan anahtar değerlerinden biri şifreleme anahtarı olarak kullanılmıştır. Çalışma sonunda, şifreleme algoritması içerisinde, açık metni şifrelemek için kullanılacak olan yeni anahtar değerlerinin üretiminde AES algoritmasının KASUMI algoritmasına oranla güçlü olduğu sonucu ortaya çıkmıştır. Çalışmada ayrıca yüksek randomizasyon veren anahtar değerlerinin kullanımı ile yapılan şifreleme işlemi sonucuna göre 3G teknolojisi içerisinde yer alan KASUMI ve AES şifreleme algoritmalarının eşit derecede şifreleme gücüne sahip olduğu ortaya çıkmıştır.
***** Bu çalışma "Mobil İletişim Teknolojilerinin Yapısı ve Bu Teknolojilerde Kullanılan Veri Şifreleme Algoritmalarının Güvenirliklerinin Analizi" adlı doktora tezinden üretilmiştir.

**Anahtar kelimeler:** Güvenlik, Mobil iletişim, KASUMI, AES, NIST testleri

## INTRODUCTION

Due to development in science and technology, mobile communication systems in which users have the freedom of acting independently from time and space has occurred. Hardship and restrictions of cabled communication system accelerated shifting towards mobile communication system which enables wireless communication among people. The popularity and availability of wireless communications, particularly cellular, continues to grow rapidly world-wide. Mobile users are interested in services such as mobile shopping, mobile banking and mobile payments. Multimedia applications, high data rate, mobility, and cost make wireless communication one of the most useful means of communication (Schoinas, 2013). Protecting analogue information against eavesdropping is not easy but digital transmission allows for excellent level of protection. Encryption is the process where a series of bits are transformed by mathematical or logical functions into another series of bits (Payal, 2014).

In mobile communication technology, authentication algorithms and data encryption algorithms are used on the system in order to enable secure communication of users. In this way it was aimed to prevent stealing or changing data or communicating with fake users. Encryption is an essential process to ensure confidentiality over wireless channels, because wireless channels are an open medium to intruders in which they can intercept and alter the content of any transmitted information. (Zibideh & Matalgah, 2015). Encryption is carried out in order to hide a

text, voice or image for security. Plain text, encryption code and encryption algorithm is required in order to do encryption (Babbage, 2000; Balani, 2007; Chen & Guizani, 2006). The Third Generation (3G) proposal for cellular communication aimed at maintaining compatibility with Global System for Mobile Communication (GSM) as well as address security weaknesses of the GSM architecture (Schoinas, 2013).

While UMTS (Universal Mobile Telecommunications System) system which is one of 3G (3rd Generation) mobile communication technology uses KASUMI algorithm that has block cipher structure; CDMA2000 (Code Division Multiple Access 2000) system which is also called as 3G mobile communication technology uses AES (Advanced Encryption Standard) algorithm that also has block cipher structure (3GPP Task Force, 1999; Nyberg, 2004, Fibs 197, 2001). In our study, we studied data encryption reliability of both KASUMI and AES encryption algorithms with the help of NIST (National Institute of Standards and Technology) tests (Demirkol, 2007; Akyıldız et al., 2004; Bassham, 2010; Yalcin, Suykens & Vandewalle, 2004). In the practice, same text values were entered in both encryption algorithms. 10 key values were obtained in order to encrypt this text and key value which has the highest randomization among these new key values that are obtained from AES and KASUMI algorithm were taken and used in encryption.

## RELATED WORKS

There are different studies upon the power of AES and KASIMU which are encryption methods used in 3G communications. Let's review the most important ones. KASUMI algorithm is an 8 round Feistel encryption and generates 64 bit output from 64 bit input using 128 bit K key. The first serious attack was done for KASUMI by Mark Blunden and Adrian Escott in 2002. They have done "related key" attack on 5 and 6 round KASUMI and succeeded in obtaining the key (Blunden & Escott, 2002). In 2005, Tanaka, Sugio and Kaneko applied differential cryptanalysis which uses efficiently chosen plain texts for 5 round KASUMI and they succeeded as well (Tanaka, Sugio & Kaneko, 2005). In another study carried out in the same year, Biham, Dunkelman and Keller did "Related-Key Rectangle" attack on full round KASUMI which is also successful theoretically (Biham, Dunkelman & Keller, 2005). In 2010, Dunkelman, Keller and Shamir attained 128 bit key for full round KASUMI by using only 4 related key with a recently designed attack which they named sandwich attack. They have done this attack with standard optimization parameters of gcc 4.3.2. Compiler on GHz, 4 MB L2 Cache, 2 GB RAM" and "T7200 Intel Core Duo 2 CPU and Linux-2.6.27 kernel" (Dunkelman, Keller & Shamir, 2010). As a result of this attack, the reliability of KASUMI has become problematic today. In 2014, Wang et al. DFA attacked on KASUMI-64 which is the base of A5/3 cryptosystem. They showed that only one 16-bit word fault is enough to perform a successful key recovery attack. They emphasized that when applying KASUMI-64, the last two rounds should be specially designed to protect against fault injection emphasize that when applying KASUMI-64, the last two rounds should be specially designed to protect against fault injection. In, 2014, Dunkelman, Keller and Shamir, described a new type of attack called a *sandwich attack*, and used it to construct a simple related-key distinguisher for 7 of the 8 rounds of KASUMI with an amazingly high probability of 2−14. By analyzing the single remaining round, they could derived the complete 128-bit key of the full KASUMI with a related-key attack which uses only 4 related keys. In 1997, NIST began to carry out study for an algorithm which is named AES that can be replaced with DES (Data Encryption Standard) algorithm. As a result of conferences, five finalist including Rijndael algorithm were determined in 1999 (Daemen & Rijmen, 1999). AES standard was done with fips-197 (Federal Information Processing Standards) published by NIST (Fibs 197, 2001). In 2006, "related-key impossible differential" attack was done by Biham, Dunkelman and Keller. The attack was done theoretically on the first 8 round of AES-192 using 192 bit key and it was successful (Biham, Dunkelman & Keller, 2006). In 2008, a successful "new impossible differential" attack was done by Lu, Dunkelman, Keller and Kim for 8 round AES-256 (Lu, et al, 2008). In 2010, a successful "single-key" attack was done on 10 round AES-256 by Dunkelman, Keller & Shamir. While full round AES-256 is not broken, it brings worry about the reliability of 10 round for being broken by such a trivial complexity. In 2012, "differential fault" analysis was done by Chong Hee Kim, but it was not successful for full round (Kim, 2012).

## STRUCTURE OF KASUMI ENCRYPTION ALGORITHM

KASUMI block encryption is used for reliability and protecting integrity within UMTS. KASUMI is a powerful encryption algorithm installed on MISTY1 block encryption algorithm which was designed to meet certain security, speed, and hardware complexity requirement and including 128 bit key, 64 bit block and 8 round Feistel encryption structure.Although some algorithms are widely used in wireless systems such as KASUMI, which is used in the Global System for Mobile and the Universal Mobile Telecommunications System, it is shown that this algorithm satisfy the avalanche criterion as in other traditional encryption algorithms (Zibideh & Matalgah, 2015)

Within KASUMI algorithm (Fig.1) there are 7 bit S7 and 9 bit S9 boxes which enable minimum differential and linear probability. By using S boxes in functions of each round, algorithm was enabled to be reliable against differential and linear cryptanalysis. By applying various transactions to 128 bit startup key which is entered in algorithm, new key values to be used in each round are obtained and these new key values are used in various functions. In encryption, nested functions which are different from each other such as FO, FL and FI are used. In this way, security within algorithm is improved (Balderas & Cumplido, 2004; Dohmen & Olaussen, 2001; Wang, Dong, Jia & Zhao, 2014).

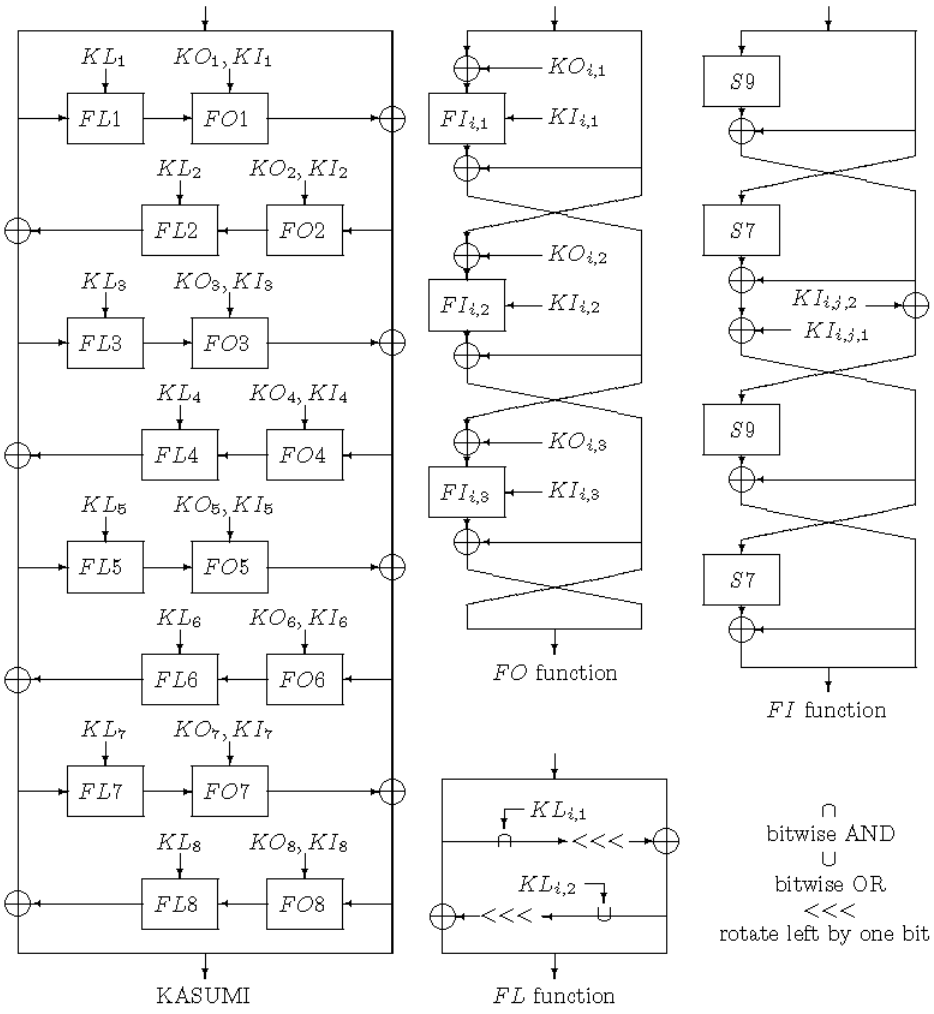


**Figure 1.** KASUMI Algorithm Flowchart (Dunkelman, Keller & Shamir, 2010).

**Obtaining Key Values**

KASUMI algorithm obtains 128 bit new key value within 128 bit key value entered in it and uses this value in the encryption. In the process of obtaining key, 128 bit key which is entered in the algorithm is separated in to 8 equals pieces, K=K1 || K2 || K3 || K4 || K5 || K6 || K7 || K8, being from j=1 to 8. $Kj_I$ sequence is obtained from Kj. For each j integer value, $Kj_I$=Kj XOR Cj keys are obtained by using 1<j<8 Cj (table 1) stable values. By using these new key values, new values to be used in different functions are obtained (Table 2).

**Table 1.** C Values

| | |
|---|---|
| C1 | 0x0123 |
| C2 | 0x4567 |
| C3 | 0x89AB |
| C4 | 0xCDEF |
| C5 | 0xFEDC |
| C6 | 0xBA98 |
| C7 | 0x7654 |
| C8 | 0x3210 |

**Table 2.** Encryption Key values

| subkeys | i.round |
|---|---|
| $KL_{i1}$ | $K_i$ <<< 1 |
| $KL_{i2}$ | $K^I_{i+2\ (\mathrm{mod}\ 8)}$ |
| $KO_{i1}$ | $K_{i+1\ (\mathrm{mod}\ 8)}$ <<< 5 |
| $KO_{i2}$ | $K_{i+5\ (\mathrm{mod}\ 8)}$ <<< 8 |
| $KO_{i3}$ | $K_{i+6\ (\mathrm{mod}\ 8)}$ <<< 13 |
| $KI_{i1}$ | $K^I_{i+4\ (\mathrm{mod}\ 8)}$ |
| $KI_{i2}$ | $K^I_{i+3\ (\mathrm{mod}\ 8)}$ |
| $KI_{i3}$ | $K^I_{i+7\ (\mathrm{mod}\ 8)}$ |

KASUMI algorithm is an 8 round Feistel encryption and generates 64 bit output from 64 bit input using 128 bit K key. FL, FO and FI functions within the algorithm form the basic structure. 64 bit value entered within algorithm is separated into two, being the first 32 bit and the last 32 bit ($L=[63:32]$ and $R=[31:0]$). We can express the algorithm as each being i, in other words round value. Fi function transforms 32 bit input value to 32 bit output value under the control of $RK_i$ round key (round key $KL_i$, $KO_i$ and $KI_i$ being triple key group). The function is obtained from two sub-functions structurally. FL and FO function are integrated with $KL_i$ (which is used with FL) and $KO_i$-$KI_i$ (which are used with FO) subkey. Fi function is formed in two ways being related to single and dual rounds (Blanchard, 2000; Kitsos, Galanis and Koufopavlou, 2004; Akleylek, 2008).

for 1, 3, 5 and 7 rounds;

$$f_i(I, RK_i) = FO(FL(I, KL_i), KO_i, KI_i)$$

for 2, 4, 6 and 8 rounds;

$$f_i(I, RK_i) = FL(FO(I, KO_i, KI_i), KL_i)$$

**Process Steps in KASUMI Algorithm**

***FL Function:***

FL Function takes 32 bit I input value and process it with 32 bit KL key value. While KL key is separated into two sub-keys being 16 bit $KL_{i,1}$ and $KL_{i,2}$, in round number; 32 bit I input value is separated into I=L||R 16 bit two groups. The processes below are done and 32 bit output value $O=(L^I||R^I)$ is obtained (Fig.1).

$$R^I = R \oplus ROL(L \cap KL_{i,1})$$

$$L^I = L \oplus ROL(R^I \cup KL_{i,2})$$

***FO Function***

FO function includes 32 bit input data and 48 bit $KO_i$ and 48 bit $KI_i$ values; i being the round number. 32 bit input data is separated into two parts being L and R.

48 bit sub-keys are separated into three 16 bit subkeys.

$$KO_i = KO_{i,1} \| KO_{i,2} \| KO_{i,3}$$

$$KI_i = KI_{i,1} \| KI_{i,2} \| KI_{i,3}$$

Being $1 \le j \le 3$

$$R_j = FI(L_{j-1} \oplus KO_{i,j}, KI_{i,j}) \oplus R_{j-1}$$

$$L_j = R_{j-1}$$

values are obtained in each round and at the end of 3. round final value $(L_3 \,||\, R_3)$ to be.

***FI Function***

FI function uses 16 bit input value and 16 bit $KI_{i,j}$ key value. Input value is separated into two unequal parts. L0 is the first 9 bit values in the left; R0 is the first 7 bit values in the right. $KI_{i,j}$ key value is separated into two parts being 7 bit $KI_{i,j,1}$ sub-key value and 9 bit $KI_{i,j,2}$ sub-key value.

$$KI_{i,j} = KI_{i,j,1} \| KI_{i,j,2}$$

The function uses two S boxes. These are S7 box which maps 7 bit input to 7 bit output and S9 box which maps 9 bit input to 9 bit output. These boxes also use two additional functions which are called ZE() and TR().

ZE(X)= transforms 9 bit X value by adding 2 zero values to the most important part.

TR(X)= transforms 9 bit X value into 7 bit X value ignoring the most important bits.

$L_1=R_0$

$$R_1 = S9[L_0] \oplus ZE(R_0)$$

$$L_2 = R_1 \oplus KI_{i,j,2}$$

$$R_2 = S7[L_1] \oplus TR(R_1) \oplus KI_{i,j,1}$$

$L_3=R_2$

$$R_3 = S9[L_2] \oplus ZE(R_2)$$

$$L_4 = S7[L_3] \oplus TR(R_3)$$

$R_4=R_3$

The function generates 16 bit (L4 || R4) result.

**STRUCTURE OF AES ENCRYPTION ALGORITHM**

AES is one of the encryption techniques which is used most frequently because of its high efficiency and simplicity. It is the highly secure algorithm. AES represents the current recommended standard by NIST for encryptions (Kaul et al. 2015). AES (Fig.2) is an algorithm which encrypts 128 bit data blocks with 128, 192, 256 bit key choices. It is a broad type

of SPN algorithm. The number of round varies according to key width. While it encrypts 10 round for 128 bit key, it encrypts 12 and 14 round respectively for 192 and 256 bit keys. Every round is composed of four layers in AES algorithm. First of all 128 bit data is transformed to 4x4 byte matrix. Then, in each round bytes are displaced, lines are shifted, columns are compared XOR process is done with key values from key planning and determined for that round. In the displacement of bytes each of 16 byte values are entered into 8 bit input and 8 bit output S box. In the process of row shifting, rows are shifted in 4x4 byte matrix and in the process of column comparison values at that column are compared for any column. In the last layer of the round, encrypted data was obtained doing XOR process with key values of that round (Chung & Phan, 2002; AES, 2001).

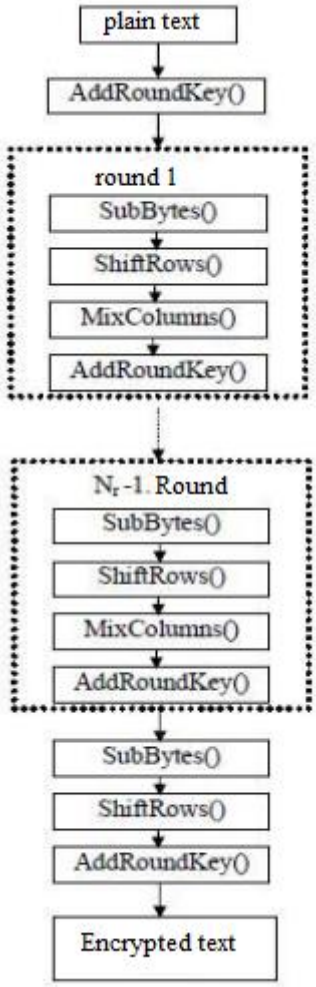


**Figure 2.** AES Algorithm Flowchart

**Obtaining Key Values**

AES encryption algorithm tries to encrypt 128 bit block data with 128 bit key value. In the beginning of encryption process, new key values are obtained from current 128 bit key values. The first 128 bit key value is divided into 4 blocks in itself. These four blocks are entered into Key Extension algorithm. Data are shifted to the left in key extension algorithm, entered into S boxes and treated with XOR process with some specific stable values. As a result, new different key values are obtained in order to use at each round of AES encryption algorithm (Fibs 197, 2001).

**Sub-Bytes Function**

It is a layer where S box is used. It takes the information of input matrix and passes each byte through a defined S box and obtains result. In the displacement of bytes, each 16 byte values are entered into 8 bit input and 8 bit output S box. After S box values are negated in Galois field (Galois Field - GF) GF(28), for 8 bit polynomial (m(x) = x8 + x4 + x3 + x + 1) it is obtained by entering a linear transformation. In this way inverse of each byte are found in the matrix.

**Shift-Rows Function**

This function takes condition matrix and shifts the last three rows to the left circularly according to specific values. In the process of shifting, while the 1st row remains same, 2nd row is shifted one time, 3rd row is shifted two times and 4th row is shifted 3 times.

**MixColumn Function**

This function takes condition matrix and shifts the last three rows to the left circularly according to specific values. In the process of shifting, while the 1st row remains same, 2nd row is shifted one time, 3rd row is shifted two times and 4th row is shifted 3 times.

**AddRound Key Function**

In this function, every round value is treated with XOR process with new key values obtained for them.

## RANDOM NUMBER GENERATOR

Randomization is observed as a feature where there are not simple relations between elements, there is no specific draft, in short as inestimable feature. Randomization is one of the most common features used in order to enable privacy, dissolution in cryptography. The result of encryption should be as much inestimable as it can be in order for the attacker not to obtain actual data. Random numbers form the basis of many cryptographic practices. There are random number generators in order to use in cryptographic practices. Numbers in the output of random number generator are systems which are statistically independent from each other. It is possible to divide random number generators (RNG) into two such as actual random number generators (ARNG) and pseudo random number generators (PRNG). One of them is preferred according to the aim of practice. While the practice of actual RNG depends on the

measurement of national process such as noise, pseudo RGN uses deterministic processes such as digital algorithms (Grošek, Vojvoda & Krchnav, 2009).

**Statistical Tests for Random Number Generators**

These tests tell us whether the output of the generator fulfills the requirements expected from a random series. Moreover, the quality of random number generator can be commented considering test results. In order to say whether a number sequence is random or not, it must be tested. If only one test is unsuccessful the sequence is not accepted to be random. Statistical hypothesis test are used in order to do statistical deduction. A hypothesis (null hypothesis, H0) is put forwards in these tests, the inverse of this hypothesis is accepted to be alternative hypothesis, Ha. There are two different decisions to be attained as a result of statistical test: *Reject or not reject H0.*

The first decision is taken when there is a strong proof against H0. When this strong proof is not found, the second decision is taken. There is an inevitable factor of error in all statistical tests. Two different types of error, first type (alpha) error and second type (beta) error can be made as a result of the test. The first type of error happens when the decision is reject H0 while hypothesis is correct. The second type of error happens when the decision is not reject H0 while hypothesis is false. The probability of making first type error should be restricted in the hypothesis test. The probability of making first type error gives the reliability level of our test. This value is generally chosen as 0.01-0.05. The power of a statistical test is equal to the probability of not making second type error. More sampling is carried out in order to increase the power of test. While doing a statistical test; first of all H0 and Ha are determined. Then, reliability level of the test is determined. A sampling is done and test statistics and p-value related with it are calculated. Instead of controlling the probability of making first type error, p-value corresponds to the probability of test statistics being an observation value or more extreme value, on the assumption that H0 is correct. The probability which is calculated according to this definition gives p-value. If this value is smaller than the chosen reliability value H0 hypothesis is rejected. Distributions which are most commonly used in statistical tests are Normal and Chi-square distributions (Akyıldız, et al, 2004).One of the common tests is NIST 800-22 (Bassham, 2010) which are published by Institute of National Standards and Technology. This test system is generally formed in order to test data which are composed of long blocks.

**NIST 800-22 Test System**

The system is used in order to test data which are composed of long blocks. It has more powerful structure compared to previous tests. In other words, a system which had passed previous tests and accepted to be reliable may not pass this test. For this reason, this system is a structure which can be used in serious processes. NIST 800-22 is composed of 15 separated tests. In order for a tested bit sequence to be successful it should pass all the tests successfully. Below are the tests with brief explanations:

**1. Frequency Test:** analyzes 1 and 0 balance in bit sequence.

**2. Block Frequency Test:** analyzes 0 and 1 balance of m bit blocks.

**3. Runs Test:** analyzes the number of 0 and 1 blocks (runs).

**4. Longest run of Ones in a Block Test:** analyzes the length of 0 and 1 blocks (runs).

**5. Rank Test:** By using bit blocks at stable lengths, creates a matrix each one of which indicating a row and calculating the rank of matrix, linear dependence between blocks are analyzed.

**6. Discrete Fourier Transform Test:** Takes Fourier transformation of current bit sequence and analyzes periodicity.

**7. Non-Overlapping Template Matching Test:** Analyzes the recurrence of m bit block within sequence. In the event of recurrence, creates a new m-bit block beginning from the recurrent block.

**8. Overlapping Template Matching Test:** Analyzes the recurrence of m bit block within sequences. In the event of recurrence, a new one is created by shifting the block 1 bit.

**9. Universal Test:** Analyzes how far the sequence could be compressed without data loss

**10. Linear Complexity Test:** Analyzes the complexity of bit sequence by observing the length of LFRS (linear feedback shift register).

**11. Serial Test:** Analyzes the number of recurrence of 2m block. For m=1, it is equal to the first test.

**12. Approximate Entropy Test:** Analyzes entropy of recurrent and m and (m+1) bit blocks.

**13. Cumulative Sums Test:** Separating bit sequence into sequential length blocks; determines 1 and 0 balance and considers the difference of unbalance between blocks.

**14. Random Excursion Test:** Separating bit sequence into sequential length blocks; determines 1 and 0 balance and then analyzes the distribution of block balance.

**15. Random Excursion Variance Test:** Separating bit sequence into sequential length blocks; determines 1 and 0 balance and determine deviation from average value.

## COMPARISON OF KEY VALUES OF KASUMI AND AES ENCRYPTION ALGORITHMS

Being the same with KASUMI algorithm used in UMTS system and AES algorithm used in CDMA2000 system; ten 16 character, 128 bit, encryption keys were entered and these 10 encryption key were transformed to be used in encryption within algorithms and randomization of the values were tested by using NIST test package (Table 3).

**Table 3**. Selected keys

| | | | |
|---|---|---|---|
| **Key 1** | Yt5D*}98?fwM2&jR | **Key 6** | ewG%33bcxfsmlk99 |
| **Key 2** | 7ygv6tfc5rdx8265 | **Key 7** | 7+Gf5/%gOpEw%'3r |
| **Key 3** | 9P^3%FaR#09hG21( | **Key 8** | FatmAakGUN128753 |
| **Key 4** | FGd&33Sx(=&fdcxs | **Key 9** | £$k9sd\ks7@nönbf |
| **Key 5** | r35+^g3ST^1F-=o4 | **Key 10** | 635Fr^2XdawN^}nS |

Following the application of test package, p-values were evaluated and stated graphically. Success value $\alpha = 0.01$ is taken as. Since program output applied to NIST test package could not meet adequate criteria for some of the test, p-values could not be obtained. Below is the table about key-value entered for the formation of new keys to be used in KASUMI and AES block encryption algorithms and probability values and their graphical values obtained as a result of applying NIST tests were given (Fig. 3, 4, 5, 6).

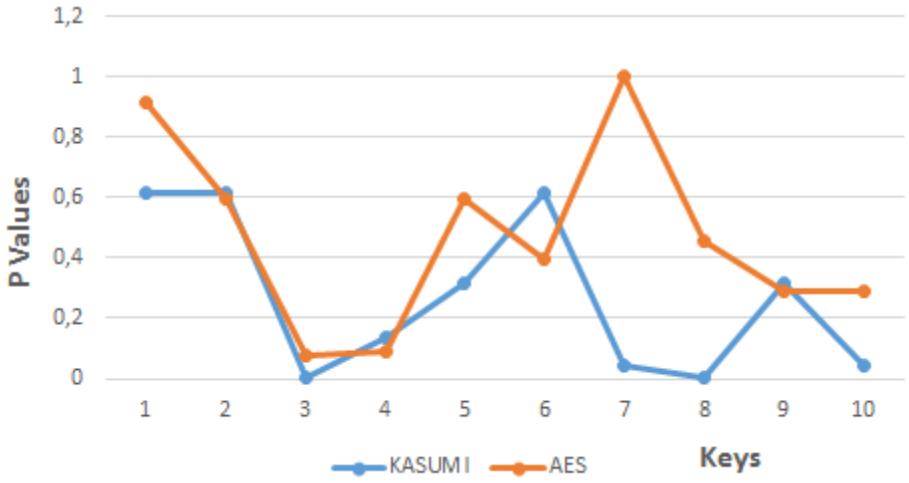


**Figure 3.** Frequency Test

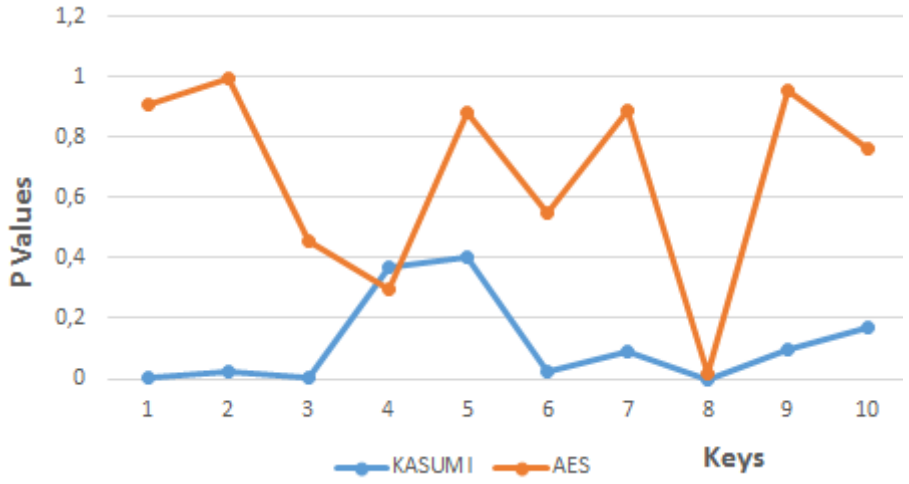


**Figure 4.** Longest run of Ones in a Block Test

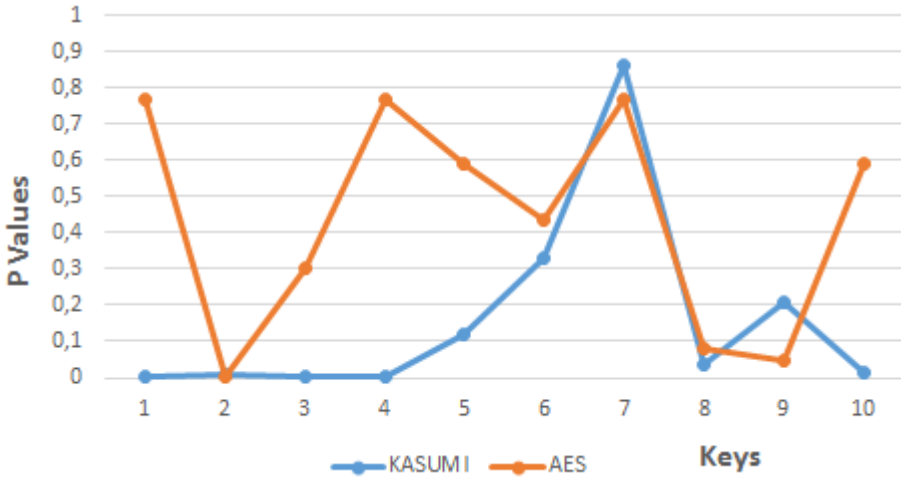


**Figure 5.** Discrete Fourier Transform Test

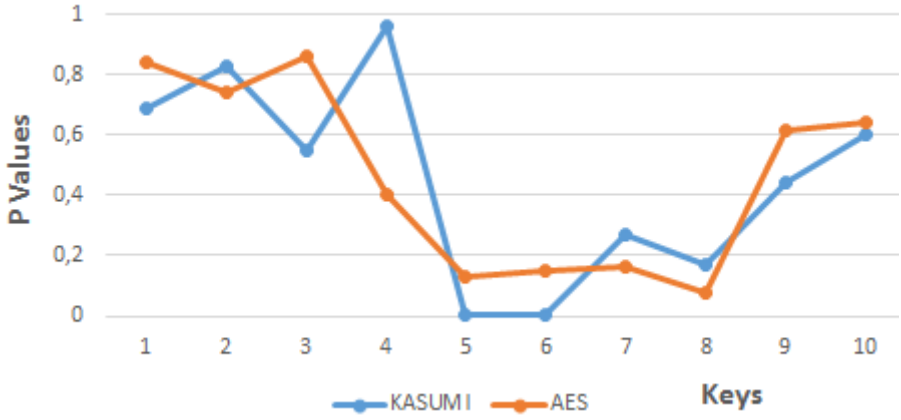


**Figure 6.** Cumulative Sums Test

As it can be observed from the graphics above; AES algorithm was more successful than KASUMI algorithm in the process of key generation. In Frequency Test and Cumulative Sums Test, 6 out of the 10 key values which were generated by AES algorithm, were more successful than the ones that are generated by KASUMI algorithm. In Discrete Fourier Transform Test, AES was better in 7 key values and In Longest run of Ones in a Block Test, it was better in 9 key values.

In the process of AES algorithm key generation, S-boxes which are reliable against linear and differential cryptanalysis were used. S-boxes (replacement boxes) are quite important since they are the only non-linear elements of block encryption algorithm. Therefore a good choice of S-box directly prevents the complexity of the cipher. Besides this, in key obtaining process, the key was made stronger by delaying rows and making XOR process by previous round keys. In KASUMI algorithm, as a result of processing new startup key value with specific values, new cycle key values are obtained. The key obtained in this way is weak.

## COMPARISON OF ENCRYPTED TEXTS OF KASUMI AND AES ENCRYPTION ALGORITHMS

A written text was ciphered by making use of NIST test results, and using **Yt5D*}98?fwM2&jR** key-value which has high randomization in KASUMI and AES encryption algorithms which use 128 bit block. Results of encryption were applied on NIST tests and graphics were drawn for result values of each test (Fig.7, 8, 9, 10).

As a result of NIST tests, key values which have the highest randomization for both encryption algorithms were chosen and a written text was encrypted and NIST tests were applied to the encrypted text. Again depending on NIST test results, it was observed that randomization of encrypted texts generated by both AES and KASUMI encryption algorithms were at the same levels and they have different superiorities over each other in NIST test samplings.

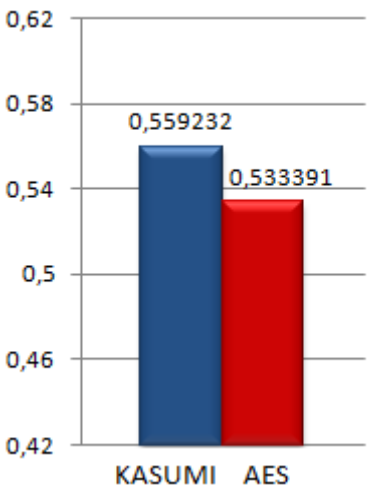


**Figure 7.** Frequency Test

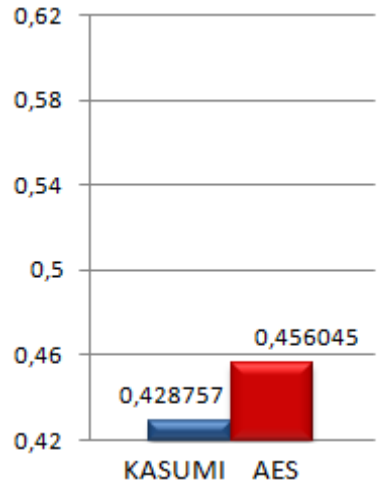


**Figure 10.** Discrete Fourier Transform Test

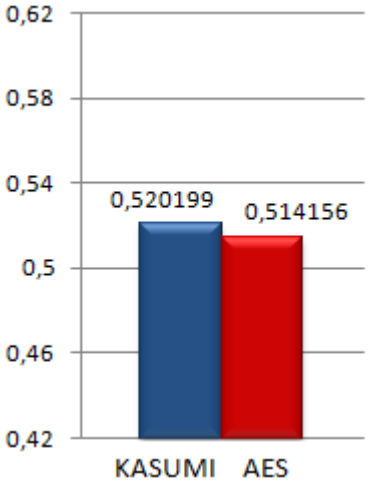


**Figure 8**. Runs Test

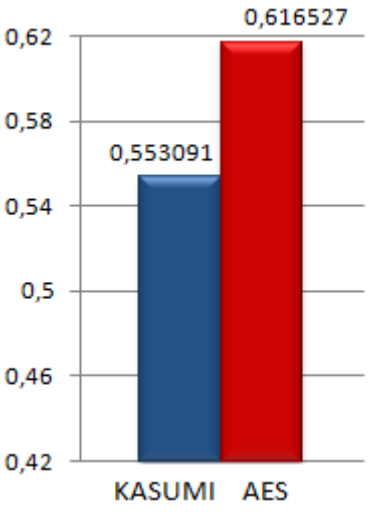


**Figure 9.** Longest run of Ones in a Block

## CONCLUSIONS

In mobile communication technology, authentication algorithms and data encryption algorithms are used to provide secure communication between users. So in this study, the power of data encryption algorithms used in UMTS and CDMA2000 systems which are 3G mobile communication technologies were analyzed. A key value among 10 key values generated from AES and KASUMI algorithms which is observed to give good results from NIST test used for both algorithms was taken and encryption was done by using written text statement. In the applications, new key values to be used for data encryption are generated and these key values are tested by using test package of NIST in order to check whether these key values are generated randomly or not; and then one of the key value which has high randomness is used as encryption key and thereafter again NIST test package is used for testing whether acquired encrypted text values are random or not. Including the acquired test criteria results, evaluations are made on the power of encryption algorithms used in mobile communication technologies. When we apply NIST tests on key values obtained as a result of both algorithms, it was also observed from the graphic above that new key values to be used in AES algorithm have higher randomization, in other words they are more complex and reliable compared to key values to be used in KASUMI algorithm. It was observed that both algorithms have similar power in obtaining encipher text. With the results obtained, the problem of KASUMI in key generating should be reviewed. As a result, both methods have similar power when powerful keys are selected and the obtained results are shown graphically.

## REFERENCES


1. 3GPP Task Force. Document 2: KASUMI specification: 3GPP confidentiality and Integrity Algorithms, 1999.
2. ADVANCED ENCRYPTİON STANDARD (AES), *Federal Information Processing Standards Publication 197,* November 26, 2001.
3. AKLEYLEK, S. On The Avalanche Properties of Misty1, Kasumi and Kasumi-R. A Thesis Submitted To The Graduate School of Applied Mathematics of Middle East Technical University, 2008.
4. AKYILDIZ, E., DOĞANAKSOY, A., KEYMAN, E. ve UĞUZ, M. *Kriptolojiye Giriş Ders Notları*. Uygulamalı Matematik Enstitüsü, Kriptografi Bölümü, ODTÜ, TÜRKİYE, 115-120, 2004.
5. BABBAGE, S. Design of Security Algorithms for Third Generation Mobile Telephony, Vodafone Ltd, *Information Security Technical Report*, 5(3), 66-73, 2000.
6. BALANI, A. Authentication and Encryption in CDMA Systems. Head-India Carrier Support Group, LG Soft India Private Limited, 2007.
7. BASSHAM, L, E. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. *NIST Special Publication 800-22,* Computer Security, April 2010.
8. BIHAM, E., DUNKELMAN, O. and KELLER, N. Related-Key Impossible Differential Attacks on 8-Round AES-192. *CT-RSA 2006*, LNCS 3860, pp. 21-33, 2006.
9. BIHAM, E., DUNKELMAN, O. and KELLER, N. Related-Key Rectangle Attack on the Full KASUMI. *Asiacrypt 2005*, LNCS 3788, pp. 443-461, 2005.
10. BLANCHARD, C. Security for the Third Generation (3G) Mobile System, *Information Security Technical Report,* 5(3), pp.55-65, 2000.
11. BLUNDEN, M. and ESCOTT, A. Related Key Attacks on Reduced Round. *LNCS*, Vol.2355, 277-285, 2002.
12. CHEN H. H. and GUIZANI M. Next Generation Wireless Systems and Networks, *John Wiley & Sons*, ISBN- 13 978 -0-470-02434-8 (HB), 2006.
13. CHUNG, R. and PHAN, W. Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students. *Cryptologia*, 26(4), 283-306, 2002.
14. BALDERAS, T. and CUMPLIDO, R. An Efficient Hardware Implementation of the KASUMI Block Cipher for Third Generation Cellular Networks. *In: Proc. GSPx,* 2004.
15. DAEMEN, J. and RIJMEN, V. AES Proposal: Rijndael, Document version 2, 1999.
16. DEMIRKOL, A.Ş. Kaotik Osilatör Girişli Adc Tabanlı Rastgele Sayı Üreteci, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Basılmamış Yüksek Lisans Tezi, 2007.
17. DOHMEN J. R. and OLAUSSEN L. S. UMTS Authentication and Key Agreement. Graduate Thesis, Agder University College, Grimstad - Norway, 2001.
18. DUNKELMAN, O. KELLER, N. and SHAMİR, A. A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. *Journal of Cryptology*, 824–849, 2014.
19. DUNKELMAN, O., KELLER, N. and SHAMIR, A. A practical-time attack on the KASUMI cryptosystem used in GSM and 3G telephony. *Crypto 2010*, LNCS 6223, pp. 393-410, 2010.
20. DUNKELMAN, O., KELLER, N. and SHAMIR, A. Improved Single-Key Attacks on 8-Round AES-192 and AES-256. *ASIACRYPT 2010:* 158-176, 2010.
21. FIPS 197. November 26, 2001 Advanced Encryption Standard, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C.
22. GROŠEK, O., VOJVODA, M. and KRCHNAV, R. A new matrix test for randomness. *Computing*, 85:21–36, 2009.
23. KAUL, V., BHARADI, V. A., CHOUDHARI, P., SHAH, D. and NARAYANKHEDKAR, S. K. Security Enhancement for Data Transmission in 3G/4G Networks, *International Conference on Computing Communication Control and Automation*, 2015.
24. KIM, C. H. Improved Differential Fault Analysis on AES Key Schedule. *IEEE Transactions on Information Forensics and Security*, 7(1), 2012.
25. KITSOS, P., GALANIS, M.D. and KOUFOPAVLOU, O. High-Speed Hardware Implementations of the Kasumi Block Cipher. *Circuits and Systems-ISCAS '04*, Vol 2. 549-52, 2004.
26. LU, J., DUNKELMAN, O., KELLER, N. and KIM, J. New impossible differential attacks on AES, *Indocrypt 2008*, LNCS 5365, 279-293, 2008.
27. NYBERG, K. Cryptographıc Algorithms for UMTS. *European Congress on Computational Methods in Applied Sciences and Engineering*, ECCOMAS 2004, 8-13, 2004.
28. PAYAL, V. N. GSM: Improvement of Authentication and Encryption Algorithms. *International Journal of Computer Science and Mobile Computing*, 3(7), 393-408, 2014.
29. SCHOINAS, P. Secure military communications on 3G, 4G and WiMax. Naval PostGraduate School, Monterey, California, Thesis, 2013.
30. TANAKA, H., SUGIO, N. and KANEKO, T. A Study on Higher Order Differential Cryptanalysis of 64 bit block cipher Kasumi. *Journal of the National Institute of Information and Communications Technology*, Vol.52, 129-134, 2005.
31. WANG, Z., DONG, X., JIA, K. and ZHAO, J. Differential Fault Attack on KASUMI Cipher Used in GSM Telephony. *Hindawi Publishing Corporation Mathematical Problems in Engineering*, Article ID 251853, 2014.

32. YALÇIN, M. E., SUYKENS, J. A. K. and VANDEWALLE, J. True Random Bit Generation From a Double-Scroll Attractor. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 51 Issue: 7, 1395 - 1404, 2004.

33. ZIBIDEH, W. Y. and MATALGAH, M. M. Modified Data Encryption Standard Encryption Algorithm with Improved Error Performance and Enhanced Security in Wireless Fading Channels. *Security and Communıcatıon Networks*, 565-573, 2015.