ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Improved Protection Measures in WEP/WPA/WPA2-PSK using Random Bitwise Signatures

BabitaDagar, Neha Goyal

M.Tech (pursuing), Dept. of Computer Science, Shri. Ram College of Engineering and Management, Palwal, Haryana under the Affiliation of Maharshi Dayanand University, Rohtak, India

Assistant Professor, Dept. of Computer Science, Shri. Ram College of Engineering and Management, Palwal, Haryana under the Affiliation of Maharshi Dayanand University, Rohtak, India

ABSTRACT:Random Bitwise Signature is a modification of Digital Signature. The conception of Random Bitwise signature is that the requester enables to derive the signature but the signer disables to link a pair of signatures. This study proposes an improved Random Bitwise signature scheme with high security and improved performance.

KEYWORDS:Random Bitwise Signature, Digital Signature, Discrete Logarithm Problem

I. INTRODUCTION

A Digital Signature Scheme is a mathematical scheme that exhibits the authenticity of a sender. A valid digital signature provides a recipient to ensure that the message was created & sent by a known sender. Digital Signatures are commonly used for software distribution, financial transactions, financial transactions, electronic voting and in other situations where it is important to detect forgery or tampering. Along with authentication, digital signature also possesses the property of integrity. Due to its importance and in order to use it in various kinds of applications, many types of digital signature scheme has been proposed. Random Bitwise Signature is one of them.
In the field of Cryptography, A Random Bitwise signature scheme was first introduced by David Chaum is a variant of digital signature scheme in which the content of message is Random Bitwise before it is signed. The resulting Random Bitwise signature can be publicly verified against the original un Random Bitwise message. The Random Bitwise A Digital Signature Scheme is a mathematical scheme that exhibits the authenticity of a sender. A valid digital signature provides a recipient to ensure that the message was created & sent by a known sender. Digital Signatures are commonly used for software distribution, financial transactions, financial transactions, electronic voting and in other situations where it is important to detect forgery or tampering. Along with authentication, digital signature also possesses the property of integrity. Due to its importance and in order to use it in various kinds of applications, many types of digital signature scheme has been proposed. Random Bitwise Signature is one of them.
In the field of Cryptography, A Random Bitwise signature scheme was first introduced by David Chaum is a variant of digital signature scheme in which the content of message is Random Bitwise before it is signed. The resulting Random Bitwise signature can be publicly verified against the original un Random Bitwise message. The Random Bitwise Signature can protect people's privacy within a network, especially in an electronic user payment system or electronic voting system. In the digital signature scheme, there are two participants, namely the signer & the verifier. The signer first uses a private key to sign a message and then sends this signature to the verifier. After the verifier receives the signature, he/she can use a public key to verify the legitimacy of the signature. On the other hand, in Random Bitwise signature scheme, there are three participants, namely, the requester, the signer and the verifier. Firstly, the requester Random Bitwises the message and sends the Random Bitwise message to the signer. After receiving the Random Bitwise message, the signer can use a private key to sign it and sends the Random Bitwise signature back to the requester. When the requester receives it, he/she unRandomBitwises the Random Bitwise signature to obtain the

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

signature and sends it to the verifier. When the verifier receives it, he/she can use a public key to verify the legitimacy of the signature.
The major difference between the digital signature and the Random Bitwise signature are as follows [1, 2].

i. In the Random Bitwise signature scheme, the content of the message should be Random Bitwise to the signer.
ii. When the message-signature pair is known to public, the signer should not be able to trace the message-signature pair.

The Random Bitwise signature schemes must meet the following requirements, namely, correctness, Random Bitwiseness, unforgeability, untraceability. These requirements are explained as:
Correctness:-The correctness of the signature of a message signed through the signature scheme can be checked by anyone using the signer's public key.
Random Bitwiseness:-The content of the message should be Random Bitwise to the signer.
Unforgeability:-Only the signer can give a valid signature for the associated message.
Untraceability:-The signer of the Random Bitwise signature is unable to link the message-signature pair even when the signature has been revealed to the public.

II. LITERATURE REVIEW

This section provides a review of the literature on evolution of security protocols for Wireless LAN in order to achieve requirements of confidentiality, data integrity and authentication. The encryption/decryption process, limitations and the vulnerability of each protocol to various attacks have been provided in this section.

Wired Equivalent Privacy
Wired Equivalent Privacy (WEP) was the first protocol for securing wireless network and was introduced in September 1999 as part of IEEE 802.11 security standard. The purpose of Wired Equivalent Privacy (WEP) was to provide security comparable to that of wired networks. RC4 stream cipher is used by WEP to provide confidentiality and CRC-32 for data integrity. The standard specified for WEP provides support for 40 bit key only but non-standard extensions have been provided by various vendors which provide support for key length of 128 and 256 bits as well. A 24 bit value known as initialization vector is also used by WEP for initialization of the cryptographic key stream.

WEP Encryption process consists of following steps:

i. 24 bit initialization vector is concatenated with 40 bit WEP key.
ii. The resultant concatenated key acts as seed value for Pseudo random number generator.
iii. Integrity Algorithm CRC-32 is performed on plain text to generate Integrity Check Value (ICV) which is concatenated with plain text.
iv. RC4 algorithm is applied on Plain text + ICV and Key sequence to generate cipher text.
v. The payload for the wireless MAC frame is created by adding the IV to front of the encrypted combination of data and ICV along with other fields.

WEP Decryption Process consists of following steps:

i. Initialization vector from 802.11 frame payload is concatenated with WEP key. This acts as seed value for Pseudo Random Number Generator.
ii. CR4 algorithm is applied to cipher text of frame payload and key sequence to get plain text.
iii. Plain text and original ICV are obtained.
iv. Plain text is input to Integrity algorithm to generate new ICV.
v. New ICV is compared with original ICV to get the result.

1) WEP Shortcomings

The WEP limitations are as follows: Weak Cryptography, Absence of Key Management, Small key size, Reuse initialization vector, Lack of Replay protection, Authentication issues, Jamming, Packet Forgery, Flooding.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

2) WEP Attacks

Chopchop Attack, Bittau's fragmentation Attack, Fluhrer, Mantin and Shamir (FMS) Attack, Pyshkin, Tews and Weimann (PTW) Attack

Wi-Fi Protected Access

In order to overcome the flaws of WEP, **Wi-Fi Protected Access (WPA)** was introduced in 2003 by the Wi-Fi (Wireless Fidelity) alliance. WPA implements majority of the IEEE 802.11i standard, thus it is an intermediate solution. WPA was intended to address the WEP cryptographic problems without requiring new hardware.

1) WPA Encryption Process

WPA uses Temporal Key Integrity Protocol (TKIP) for encryption. A new key is dynamically generated for every packet; 128 bit per packet key is used. Michael algorithm is used by TKIP to generate Message Integrity Code (MIC) which provides enhanced data integrity as compared to CRC-32 used in WEP. Also, TKIP provides replay protection. MSDU is Medium Access Control Service Data Unit and MPDU is Medium Access Control Protocol Data Unit.

2) WPA Authentication Mechanism

The two authentication mechanisms provided by WPA are:

i. WPA-Personal or WPA-PSK (Pre-Shared Key)

ii. WPA-Enterprise

3) WPA Shortcomings

i. WPA uses old cryptography algorithm RC4 instead of superior Advanced Encryption Standard (AES).
ii. WPA is vulnerable to brute force attacks in case of weak passphrase for pre shared key mode.
iii. Prone to threats during Hash collisions due to use of hash functions for TKIP key mixing.
iv. Also, WPA remains vulnerable to availability attacks like Denial of Service.
v. WPA has greater performance overhead unlike WEP.
vi. Complicated setup is required for WPA-enterprise.

3) WPA Attacks

TKIP used in WPA is prone to Chopchop, Ohigashi-Morii, WPA-PSK and Beck-Tews attack

II. RELATED WORK

In this section, the review of the literature, the hash function [3], the concept of Random Bitwise signature [1] and other related Random Bitwise signature schemes are introduced.

A. Cryptography:-Cryptography can be defined as the practice & study of techniques of converting meaningful text into unintelligible form. Here, the meaningful information which gets converted is called as the plain text & the unintelligible output is called the cipher text. This technique of conversion is known as encryption, while the reverse technique of retrieving the original text from the cipher text is called as decryption & aimed at achieving, mainly, confidentiality, But, in the modern era, with the development of technology as well as needs of many applications, this field has expanded to include the properties of integrity, non-repudiation, authentication etc.along with confidentiality. There are two variants of cryptography:

i. Symmetric-key cryptography
ii. Asymmetric-key cryptography

Symmetric-key Cryptography:-In this type of cryptography, the same key is shared between the sender & the receiver & used for data transmission between the two. This means that the key used by the sender to encrypt the message is also used by the receiver to decrypt the message.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Asymmetric-key Cryptography:-In this type of cryptography, instead of one key, two keys are used, one is called the public key & the other is called the private key. Here the sender uses the public key of the receiver to encrypt the message & sends it to the receiver, which is then, decrypted using his private key in order to obtain the original message. This technique is also called the Public Key Cryptography.

Cryptanalysis:-Cryptanalysis is the study of methods to obtain the meaning of encrypted information, without requiring the access to the private parameters. Cryptanalysis is also used to refer to any attempt to overcome the security of any cryptographic algorithm.

B. Services of Cryptography:-The various services provided by cryptography include:

i. Data Confidentiality
ii. Authentication
iii. Data Integrity
iv. Non-repudiation

Data Confidentiality:-International Organization for Standardization (ISO) in ISO-17799 defined confidentiality as "ensuring that information which is accessible only to authorized users".

Authentication:-This service gives a proof of authentication of the sender to the receiver or vice-versa. In peer entity authentication, during the connection establishment phase of connection oriented communication, it provides the authentication of the sender or receiver. In data origin authentication i.e. in connection-less communication, it authenticates the source of data.

Data Integrity:-Data integrity is required to protect data from unauthorized insertion, deletion, modification & replaying by an attacker. It can protect the total message or the part of message.

Non-repudiation:-To avoid repudiation (denial) by either the sender or the receiver of the data, Non-repudiation service is admissible. In Non-repudiation, the sender can confirm the delivery to the receiver with the real proof of delivery. This security service is extensively used in the verification phase of digital signatures.

C. Hash Function:-The hash function plays an important role in modern cryptography. A Cryptographic hash function is a hash function, that is, an algorithm that takes an arbitrary block of data & returns a fixed-size bit string, the hash value, such that, any change to the data will change the hash value. The data to be encoded is called the "message" & the hash value is sometimes called the "message digest" or simply "digests". Public Cryptosystem always use the hash function. By using the hash function in public Cryptosystem, it can reduce the computation time & increase the efficiency. Therefore, the hash function also plays an important role in the Public Cryptosystem, Digital Signature & Random Bitwise Signature.

D. Random Bitwise Signature:-Dr.D.Chaum introduced the concept of the Random Bitwise signature [1] in 1983. The Random Bitwise signature was a special form of digital signature because, unlike a normal digital signature scheme, the signer did not know the concept of message in the signing phase. As the Random Bitwise signature could meet the following requirements, namely, correctness, Random Bitwiseness, unforgeability&untraceability, the Random Bitwise signature could protect people's privacy in the network transaction.

E. The Concept of Random Bitwise signature:-Dr.D.Chaum was the first scholar to proposed the concept of Random Bitwise signature scheme in 1983[1]. Random Bitwise Signatures are used when you want someone to sign something but you don't want them to see what they are signing. This is done by multiplying the message by a secret number (called Random Bitwiseing). Suppose Alice wants Bob to sign a message m, but does not want Bob to know the contents of the message. Alice 'Random Bitwises' the message m, with some random number b (the Random Bitwiseing factor). This results in Random Bitwise (m, b). Bob signs this message, resulting in sign (Random Bitwise (m, b), d), where d is Bob's private key. Alice then unRandomBitwises the message using b, resulting in unRandom Bitwise (sign (Random Bitwise (m, b), d), b). This results in sign (m.d) i.e. Bob's signature on m

F. The Random Bitwise Signature based on factoring problem:-In 1976, Dr.W.Diffie and Dr.M.Hellman proposed the concept of a public key cryptosystem [4]. Factoring problems or discrete logarithms are the base for the public cryptosystem. RSA public cryptosystem is based on factoring problem.RSA is the first Random Bitwise signature introduced by Dr.DavidChaum in 1983. Suppose e is the public RSA exponent, d is the secret RSA exponent & N is the RSA modulus. Select random value r, such that r is relatively prime to N i.e. gcd(r, N) =1. r^e mod N is used as a Random Bitwiseing factor. The author of the message computes the

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

product of the message & Random Bitwiseing factor i.e. $m' \equiv m\ r^e \pmod N$ & sends the resulting value m' to the signing authority. Since r is random value. Therefore r^e mod N is random too. This implies that m' does not leak any information about m. The signing authority then calculates the Random Bitwise signature S' as:

$S' \equiv (m')^d \pmod N$. S' is sent to the author of the message, who removes the Random Bitwiseing factor, to reveal S, the valid signature of m:

$S \equiv S'.\ r^{-1} \pmod N$

Since $r^{ed} \equiv r \pmod N$

Therefore $S \equiv S'.\ r^{-1} \equiv (m')^d\ r^{-1} \equiv m^d\ r^{ed} r^{-1} \equiv m^d\ r\ r^{-1} \equiv m^d \pmod N$. Hence S is the signature of m. In RSA, the signing process is equivalent to decrypting with the signers secret key. This is known as RSA Random Bitwiseing attack.

G. The Random Bitwise signatures based on discrete logarithm problem:-J. L. Camenisch, J. M. Priveteau and M. A.Stadler first proposed the Random Bitwise signature based on discrete logarithm problems in 1994[5]. Discrete logarithm is the basis for the Elgamal public cryptosystem.

Initialization phase: The signer selects a big prime p, a prime factor q of p-1, and g, where g is a primitive root of p. He chooses a random number x, where $x \varepsilon Z_q$. He then computes y, where $y = g^x \bmod p$. The signer gets a private key x and a public key y.

Random Bitwiseing phase: The requester sends a request to the signer. After receiving the request, the signer randomly chooses a number ã, where $\tilde{a} \varepsilon Z_q$. He then computes $\check{R} = g^{\tilde{a}} \bmod p$ and checks gcd ($\check{R}$,q). If gcd ($\check{R}$, q) = 1, he sends $\check{R}$ to the requester, otherwise he must choose another ã. When the requester receives the value $\check{R}$, he must check if gcd ($\check{R}$, q) = 1. Then he randomly chooses α, β ε $Z_q$and computes $R = \check{R}^{\alpha} g^{\beta} \bmod p$.The requester checks gcd(R,q). If gcd(R, q) =1, then he computes $m' = \alpha m \check{R} R^{-1} \bmod q$ and sends m' to the signer.

Signing phase: After receiving m', the signer computes $s' = \tilde{a}m' + \check{R}x \bmod q$ and sends s' to the requester.

UnRandomBitwiseing phase: When the requester receives s' from the signer, he computes $s = s'R\check{R}^{-1} + \beta m \bmod q$ and $r = R \bmod q$. Finally, the requester gets the message-signature pair (m, r, s).

Verifying phase: The verifier can use the public key to verify the legitimacy of the signature. He then computes $T = (g^s y^{-r})\ m^{-1} = g^{(s'R\check{R}-1+\beta m-xr)\ m-1} = g^{\tilde{a}\alpha+\beta} = R \bmod p$ and checks the equation $r = T \bmod q$.

The Proposed Random Bitwise Signature:-The discrete logarithm problem and the Elgamal digital signature schemes are the base for the proposed Random Bitwise signature schemes.

Algorithm:-The proposed scheme consists of the three participants, namely, the requester, the receiver, the signer & has the following five phases:

Step 1 - [Password Optional Number Generation (Production Function)]

a) - password length is calculated.

b) - the password length n-1 * n + 1 state is calculated.

c) - 0 (zero) equal to an integer which is temporary; 1 from the length of the password itself as "1" (one, adding in each step) and password for each char (character) meets with the provision of value in the ASCII table.

d) - (Password Length of - the 1 * Password Length + 1) with integer operations as a result, the length of the password itself as the first step and the number 1 (one, adding in each step) is prepared with collected.

e) - it is unique to each version of the password and the uniqueness of the procedure to prevent the emergence of an alternative to a password due to the change in the lineup is applied. The uniqueness of the procedure, starting with the first two characters of the password as the length of the password 1 (each step 1 slide) ASCII value of the sum of the first two characters, 1 modules with a total ASCII characters are inserted into the arithmetic operation and the result is transferred to an integer, and each step results by adding this integer proceeds.

(The process will take one-time password length.)

The uniqueness of the ASCII table digits are the same for consecutive passwords but still provides uniqueness. Character differences it provides. The uniqueness of the figure is just an additional bildirgeç used characters and password combination.

f) - The number of encryption as decoding result is calculated as follows.

Encryption / Decryption Number =
Temporary integer +
Password Length +
Derivatives Password Length +
Password Uniqueness Factor

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

switches with the results generated by the collection of value is produced.
Step 2 - [A, B, C, D Parameter Estimation]
A = Encryption / Total value of Resolution number
B = Encryption / Decryption should multiply the number of number value. (Excluding 0's)
C = 1 from the Encryption / Decryption number up to the number of prime numbers.
D = 1 from the Encryption / Decryption and encryption until the number / numbers with them Solving Their number is prime.
When calculating the above "T Rectangle" consists of a structure is.
The reason it's not called a square rectangle; an edge of each parameter
Represents and each being different from each other.
Step 3 - [Eight reinforced "T Rectangle" calculation procedure.]
In this step, Encryption / Decryption number with A, B, C, D, using parameters
Rectangle number 1 is raised to 8. As used herein, X, Y, Z, P each step
temporary integer registers are required.
Rectangle 1 = (X = A X B), (Y = D + 1), (Z = X + 1), (P = number mode Y), (Result = Z + P)
Quadrilateral 2 = (X = A X B), (Y = C + 1), (Z = X + 1), (P = number mode Y), (Result = z + P)
Quadrilateral 3 = (X = B XOR C), (Y = + 1), (Z = X + 1), (P = number mode Y), (Result = Z + P)
Quadrangular 4 = (X = B XOR C), (Y = D + 1), (Z = X + 1), (P = number mode Y), (Result = Z + P)
= 5 √ (X = C X A), (Y = B + 1), (Z = X + 1), (P = number mode Y), (Result = Z + P)
Rectangular 6 = (X = C X A), (Y = D + 1), (Z = X + 1), (P = number mode Y), (Result = Z + P)
Quadrilateral 7 = (X = B X D), (Y = C + 1), (Z = X + 1), (P = number mode Y), (Result = Z + P)
Quadrilateral 8 = (X = B X D), (Y = + 1), (Z = X + 1), (P = number mode Y), (Result = Z + P)
Step 4) - Crude Encryption Keys with M, N, O, P calculation parameters
! - These parameters will be produced by 32 basic encryption key.
M parameter = (A = _0 * _1), (B = Mod _5), (C-_6 + B), (Result = C)
Parameter N = (A * = _4 _5), (B = Mod _1), (C = _2 + B), (Result = C)
O Parameter = (A * = _5 _6), (B = Mod _2), (C = _3 + B), (Result = C)
Parameter P = (A * = _7 _6), (B = Mod _2), (C = _1 + B), (Result = C)
Step 5) - Created 32 Piece Essential Key to
Note: The parentheses are important. Order of operations should not be allowed.

sandBox [00] = ((((M) X (M)) + (M)) * M)
sandBox of [01] = ((((M) X (M)) + (M)) * N)
sandBox of [02] = ((((M) X (M)) + (N)) * O)
sandBox of [03] = ((((M) X (M)) + (N)) * P)
sandBox [04] = ((((M) X (N)) + (O)) * M)
sandBox of [05] = ((((M) X (N)) + (O)) * N)
sandBox of [06] = ((((M) X (N)) + (P)) * O)
sandBox of [07] = ((((M) X (N)) + (P)) * P)
sandBox of [08] = ((((N), X (O)) + (M)) * M)
sandBox of [09] = ((((N), X (O)) + (M)) * N)
sandBox [10] = ((((N), X (O)) + (N)) * O)
sandBox [11] = ((((N), X (O)) + (N)) * P)
sandBox [12] = ((((N) X (P)) + (O)) * M)
sandBox [13] = ((((N) X (P)) + (O)) * N)
sandBox [14] = ((((N) X (P)) + (P)) * O)
sandBox [15] = ((((N) X (P)) + (P)) * P)
sandBox [16] = ((((O) X (M)) + (M)) * M)
sandBox [17] = ((((O) X (M)) + (M)) * N)
sandBox [18] = ((((O) X (M)) + (N)) * O)
sandBox [19] = ((((O) X (M)) + (N)) * P)
sandBox [20] = ((((O) XR (N)) + (O)) * M)

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

sandBox [21] = ((((O) XR (N)) + (O)) * N)
sandBox [22] = ((((O) X (N)) + (P)) * O)
sandBox [23] = ((((O) X (N)) + (P)) * P)
sandBox [24] = ((((P) X (O)) + (M)) * M)
sandBox [25] = ((((P) X (O)) + (M)) * N)
sandBox [26] = ((((P) X (O)) + (N)) * O)
sandBox [27] = ((((P) X (O)) + (M)) * P)
sandBox [28] = ((((P) X (P)) + (O)) * M)
sandBox [29] = ((((P) X (P)) + (O)) * N)
sandBox [30] = ((((P) X (P)) + (P)) * O)
sandBox of [31] = ((((P) X (P)) + (P)) * P)
Step 6) - "Length Stamp" The Calculation
Length stamp encryption / decryption procedures are recalculated every run.

a). Length stamp = Encryption / Decryption Numbers
X
Outgoing Number of Entries (as a 32-bit integer) +
Information shader (1..2048 values in the address) +
Shaders Element Number (1..2048) +
Key Sequence Offers (1..32)
b). Stamp stamp Length = Length + 1
Step 8) Decryption
Inc (encryptedValue); {Made INT32 number of inputs (sandBox / 4-Byte Count =)}
Inc (keyParameter); Increase the number of shaders Element {}
Inc (let a); {On} Key Sequence
= 2048 than if keyParameter
begin
keyParameter: = 0;
end;
= 32 than if sirabilet
begin
sirabilet of: = 0;
end;
{32-bit computer processor and memory loss in more flooding
A correction is made to avoid. INT32 value of positive
more than the maximum peak value of each entry is corrected. }
if encryptedValue> = High (integer) than
begin
encryptedValue: = Abs ((encryptedValue) - (High (integer)));
end;

keyValueof: = (sifre) when X is
(encryptedValue + bilgigolgeleyic the [keyParameter] + let of keyParameter);
Inc (keyValue a); Full uniqueness of the {Length Stamp
(Theoretically) it allows. In practice, the uniqueness can be disrupted. }
{Information int32 format, length and gained thanks to its location
length unique stamp. Complicating a simple method such as X
This is one of the most fundamental factors.}
if keyValue of> = High (integer) than
begin
keyValueto: = Abs ((keyValue a) - (High (integer)));
end;

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

TMP1: = ((Knowledge) X ((keyValue of))); Encryption Step {1}
TMP2: = ((TMP1) X (anahtarkutu the [sirabilet a])); STEP 2} {Encryption
Result: = TMP2; Info Successfully encrypt {}

V.CONCLUSION

This paper mainly applies the concept of digital signature including the requirements, namely, authentication, non-repudiation & data integrity. The existing methods for Random Bitwise signature did not provide good efficiency. For this reason, in order to improve efficiency of Random Bitwise signature, this paper also meet the requirements, namely, correctness, Random Bitwiseness, unforgeability, untraceability. It is expected that the network system such as electronic voting systems & electronic cash payment system can apply the proposed Random Bitwise signature scheme

REFERENCES

[1] D.Chaum, *Random Bitwise signatures for untraceable payments*, Advances in cryptology-crypto 82, pp.199-203, 1982.
[2] D.L.Chaum, *Random Bitwise signature systems*, US Patents 4759063, 1988.
[3] J.M.Alfred, A.V.Scott&C.V.Paul, *Handbook of Applied Cryptography*, CRC Press, 1996.
[4] H.Y.Chien, J.K.Jan, & Y.M Tseng, *RSA – based partially & distributed systems*, pp.385-389, 2001.
[5] J.L.Camenisch, J.M.Piveteau&M.A.Stadler, *Random Bitwise signatures based on the disctete logarithm problem, lectur notes in computer science*, pp.428-432, 1995.
[6] S.G.Aki, *Digital signatures: A tutorial survey*, computer, vol.16, no.2, pp.15-24, 1983.
[7] L.Harn, *Cryptanalysis of the Random Bitwise signature based on the discrete logarithm problem*, IEE Electronic Letters, 1995.
[8] H.Y.Chien, J.K.Jan and Y.M.Tseng, *RSA- based partially Random Bitwise signature with low computation*, proc. of the 8 th IEEE International Conference on Parallel 7 distributed systems, 2001.
[9] Ming-Hsin Chang, I-Chen Wu, *Schnorr Random Bitwise Signature based on Elliptic Curves*, Asian Journal of Information Technology , 2005.
[10] VivekB.Kule, P.R.Paradhi, *A Software comparison of RSA & ECC*, International Journal of Computer Science & Applications, 2009.
[11] Fuh-GwoJeng, Tzer- Wng Ethen, *An ECC- based Random Bitwise Signature Scheme* ,Journal of Networks, 2010.
[12] Victor R.l.Shen, TzerShyong Chen, *A Random Bitwise Signature on discrete logarithm problem*, ICIC Inernational, 2011.
[13] Mohammad E.Emarah A.E, *A Random Bitwise signature scheme based on Elgamal signature*, IEEE,2000.
[14] B.Forozan, Cryptography & Network Security, TMH.
[15] W.Stalling, Cryptography & Network Security, Prentice Hall.