Hybrid Schnorr, RSA, and AES Cryptosystem

Jhoanne Kris P. Alegro, Edwin R. Arboleda, Marlon R. Pereña and Rhowel M. Dellosa

Abstract— For the past years, network security has been an important issue. Authentication and encryption have come up with the solutions which play an essential role in the system of information security. Schnorr, being one of the authentication algorithms available today lacks security for the message being passed from the sender to the receiver and vice versa. This paper integrates the Schnorr authentication algorithm with RSA and AES cryptosystems in order to encompass the level of security and reduce the effectiveness of the man-middle-attack on the system. In this method, the receiver uses the Schnorr algorithm to verify that the one sending him the message is the real sender. When the sender sends the message to the receiver and vice versa, the RSA algorithm will be used and the AES algorithm, specifically the S-box, will be used for the encryption of the password for the authentication process. This method reduces the risk of intrusion as the encrypted and decrypted messages are further mixed-up through the addition of other cryptosystems.

Index Terms—AES, Cryptography, Cryptosystem, Encryption, Digital Signature, RSA, Schnorr,

1 INTRODUCTION

Data communication is a critical part of our living. So, the security of information from misapplication is important. A cryptosystem characterizes a couple of information changes called encryption and decryption[1]. Information privacy and information uprightness are two of the most important elements of modern cryptography[2]. While transmitting information between two gatherings (sender and recipient) through any remote correspondence channel, privacy is given by encryption algorithm, and the verification of information is ensured by digital signatures[3]. In the conventional worldview, to accomplish both classification and credibility in any protected system, we should utilize signature took after by encryption in particular before a message is conveyed from sender to receiver[4]. Encryption is one of the essential intends to ensure the security of sensitive data. Encryption algorithm performs different substitutions and changes on the plaintext (unique message before encryption) and changes it into ciphertext (mixed message after encryption). Numerous encryption algorithms are broadly accessible and utilized as a part of data security. Encryption algorithms are characterized into two gatherings: Symmetric-key (also called secret-key) and Asymmetric-key (also called public key) encryption. Symmetric key encryption is a type of cryptosystem in which encryption and decryption are performed utilizing similar key. It is otherwise called traditional encryption[5]. In Asymmetric keys, two keys are utilized; private and public keys. The public key is utilized for encryption and a private key is utilized for decryption. Since clients tend to utilize two keys: a public key, which is known to the general population and private key which is known just to the client [6]. In like manner, authentication strategies can be categorized by private key authentication algorithms and public key digital signatures[4]. A digital signature is an instrument by which a message is validated, demonstrating that a message is certainly originating from a given sender, much like a signature on a paper archive[7]. This study aims to provide more secure authentication and encryption of information by combining Schnorr authentication algorithm, RSA encryption algorithm, and AES algorithm. The study of [22] developed an algorithm that utilized a concept on dynamic warping for indoor positioning system. Its ultimate goal is to determine if efficiency may be improve on this algorithm.

- ***Jhoanne Kris P.*** *Alegro is from Department of Computer and Electronics Engineering, College of Engineering and Information Technology, Cavite State University.*
- ***Edwin R. Arboleda*** *is from the Department of Computer and Electronics Engineering, College of Engineering and Information Technology, Cavite State University.*
- ***Marlon R. Pereña*** *is from the Department of Information Technology, College of Engineering and Information Technology, Cavite State University.*
- ***Rhowel M. Dellosa*** *is from the Computer Engineering Department, Asia Technological School of Science and Arts.*

2 TECHNICAL ASPECTS

2.1 Need for Cryptography

Cryptography gives protection and data security[8]. In this time where data has a considerable measure of significance, such strategies assume an essential part in a few fields. Ensuring access to data for reasons of security is still a noteworthy purpose behind utilizing cryptography. In any case, it is likewise progressively utilized for approval or ID, validation, and non-repudiation. The identity of email and web clients is easy to hide or copy and secure verification can give those cooperating remotely certainty that they're managing the correct individual and that a message hasn't been corrupted. Non-repudiation is an essential idea in business circumstances that aids in keeping up the position of the concurring gatherings under all conditions if there should be an occurrence of any agreement. Passwords are normal however the insurance they offer is regularly fanciful, maybe in light of the fact that security strategies inside numerous associations aren't well thoroughly considered and their utilization causes a bigger number of issues and bother than appears to be justified, despite all the trouble. Much of the time where passwords are utilized, for instance in securing word-processed records, the ciphers utilized are to a great degree lightweight and can be attacked without exertion utilizing one of a scope of freely accessible cracking programs. [9,10].

2.2 Schnorr Authentication Algorithm

Schnorr, named after its creator Claus-Peter Schnorr, is a signature scheme: the arrangement of numerical principles that connect the private key, public key, and signature together. Numerous cryptographers consider Schnorr signatures the best in the field, as they offer a solid level of precision, do not experience the ill effects of flexibility, are generally quick to authenticate, and imperatively support multi-signature: a few signatures can be totaled into a solitary, new signature[11]. An identification plan is an interactive protocol between two gatherings, a prover (P) and a verifier (V). On the off chance that the protocol is effective, then toward the end of the protocol, the verifier is persuaded he is connecting with the prover, or more accurately, with somebody who knows the private key that compares to the prover's public key [12]. The process of Schnorr is as described below:

1. Select two primes, p and q, such that q $(1 < q < p-1)$ is a prime factor of $p-1$.
2. Select a satisfying $aq \equiv 1 \pmod p$.
3. Select private key s, such that $s < q$.
4. Compute the multiplicative inverse of a using the formula $a \cdot a\text{-}1 \equiv 1 \bmod p$.
5. Compute the public key $\lambda \equiv a-s \pmod p$.
6. The sender picks r, such that $r < q$ and computes $x \equiv ar \pmod p$.
7. The receiver picks a random number t and sends it to the sender.
8. The sender computes $y \equiv r + st \pmod q$ and sends it to the receiver.
9. The receiver verifies and computes $x' \equiv ay \cdot \lambda t \pmod p$.

The authentication will be accepted as true if $x = x'$ [13].

2.3 RSA Public-Key Cryptosystem

The knowledge of the RSA public-key cryptosystem was from Diffie and Hellman, who presented the technique for the exponential key exchange. The Diffie-Hellman key exchange is the second most famous public key algorithm, after the RSA[14]. RSA is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. A client of RSA makes and after that distributes a public key in light of the two large prime numbers, alongside an auxiliary value. The prime numbers must be kept mystery. Anybody can utilize public key to encrypt a message, yet with right now distributed strategies, if public key is sufficiently large, just somebody with information of the prime numbers can decode the message. In RSA algorithm, one party utilizes a public key and the other party utilizes a private key. Every station arbitrarily and autonomously picks two large primes p and q number and multiplies them to create n=pq. This is the modulus utilized as a part of the number arithmetic calculations of the RSA. RSA has come to show an important part in electronic communications. The strength of the algorithm, the absence of thorough verification regardless, gives a sense of security. Being the primary case in history of the public key cryptosystem and the main sort that has withstood over three decades of assaults from the best cryptographic minds, the algorithm is thought to be the absolute best and the most developed public-key cryptosystem that is generally utilized as a part of different fields [15]. In this proposed work, RSA algorithm will be used to encrypt the data to provide security so that only the concerned user can access it. RSA algorithm involves three steps: key generation, encryption, and decryption The steps for implementation of the RSA algorithm are given below: Key Generation Procedure

1. Choose two distinct large random prime numbers p and q.
2. Compute n by multiplying p and q.
3. Calculate $\varphi(n) = (p-1)(q-1)$.
4. Choose e, $1 < e < \varphi(n)$, that is relatively prime to $\varphi(n)$.
5. Compute d to satisfy the congruence relation $d \equiv e\text{-}1 \bmod \varphi(n)$; d is kept as a private key exponent.
6. The public key is (n, e) and the private key is (n, d). Keep all the values p, q and $\varphi(n)$ secret

Encryption:

Assume Bob wants to send something specific (say „m") to Alice. To encrypt the message utilizing the RSA encryption scheme, Bob must get Alice's public key pair (n, e). The message should now be encrypted utilizing the pair (n, e). However, the message „m" must be characterized to as a number in the interval [0, n-1]. To be able to encrypt it, Bob essentially processes the number „c" where $c = m^e \bmod n$. Bob sends the ciphertext c to Alice [1].

Plaintext: $p < n$.
Ciphertext: $c = m^e \bmod n$.

Decryption:

To be able to decrypt the ciphertext c, Alice has to utilize her own particular private key d (the decryption exponent) and the modulus n by just calculating the value of $c^d \bmod n$ and this yield back the decrypted message (m)

Ciphertext: c
Plaintext: $m = c^d \bmod n$.

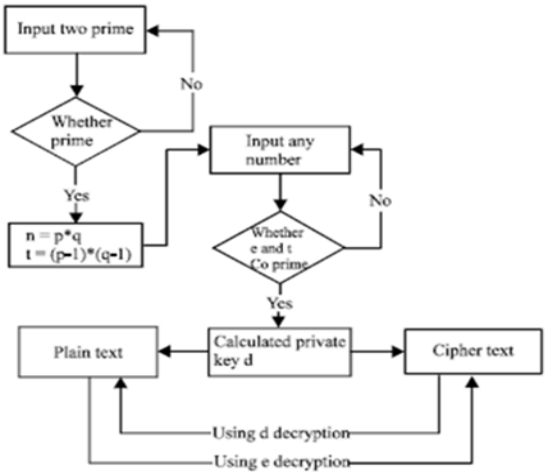

Fig 1. Flow chart or RSA.

Encryption and decryption formulas demonstrate to encode and decode a number. Greater (or diverse) bits of data are encoded by changing over them into (potentially large) whole numbers first. As RSA is not especially quick, it is normally just to encode the key of some faster algorithm. After RSA decrypts the key, this supplementary algorithm utilizes it to decrypt whatever remains of the message.

2.4. AES Algorithm

AES is short for Advanced Encryption Standard and is a United States encryption standard characterized in Federal Information Processing Standard (FIPS) 192. AES is a symmetric encryption algorithm handling information in block of 128 bits[16]. AES is symmetric since similar key is utilized for encryption and the reverse transformation, decryption. The only secret important to keep for security is the key [17, 18] The significant phase in the Advanced Encryption Standard (AES) algorithm is the "S-box". Joan Daemen and Vincent Rijimen developed the block cipher called Rijndael S-box. The algorithm supports any combination of data key size of 128, 192 and 256 bits[19]. An S-box is a coordinated mapping for all byte values from 0 to 255. The S-box is utilized to alter the first plain content in bytes to ciphertext. All values are in hexadecimal form[20].

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	3B	52	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	**2A**	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig. 2 AES algorithm S-box.

The cipher transformation can be implemented in reverse order to produce an Inverse Cipher for the AES algorithm, in which the inverse S-box is applied to each byte[21].

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	**95**	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Fig 3. AES algorithm Inverse S-box.

3 Proposed Hybrid

Since Schnorr Authentication Algorithm only verifies and authenticates the user to access certain information, the author made a solution on how to secure the message being sent and received in the system. This paper proposes a hybrid of Schnorr authentication algorithm, RSA encryption algorithm, and AES algorithm. RSA Public-key Cryptosystem will be implemented for more secure information to be given by the user to the receiver while AES will be used in the process of encryption and decryption before it will proceed to the process of authentication. S-box and inverse S-box are only part of the AES algorithm that is used in this paper. The boxes are used for the encryption and decryption of the password generated by the receiver which will be sent to the sender.

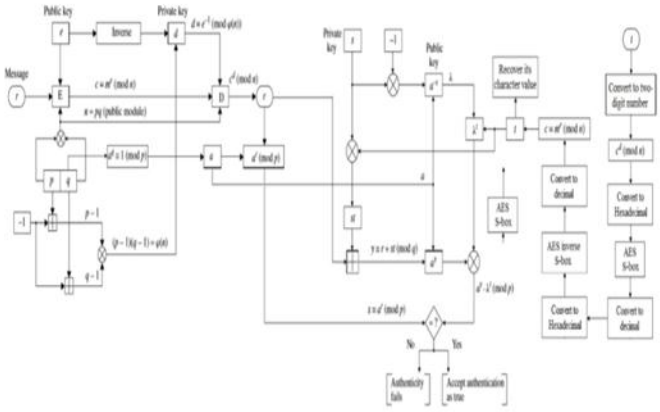

Fig. 4. Block Diagram for the Hybrid.

4 Methodology

The method for the proposed hybrid is as described below: The method starts with the process of Schnorr.

1. Choose two distinct prime numbers p and q, such that q (1 < q < p-1) is a prime factor of p-1.
2. Choose a satisfying aq ≡ 1 (mod p).
3. Choose s such that s < q.
4. Using the formula a•a-1 ≡ 1 mod p, calculate the multiplicative inverse of a.
5. Calculate λ ≡ an−s (mod p).
6. The sender selects r, such that r < q. This is where the RSA algorithm comes in. In this case, the message r that the sender selects will be them for the RSA process. r = m.
7. Calculate n = p x q.
8. Calculate φ(n) = (p-1) (q-1).
9. Select e, 1 < e < φ(n), such that e and φ(n) are coprime. 10. Calculate d satisfying the congruence relation d ≡ e-1 mod φ(n).
10. Calculate ciphertext c using the formula c = me mod n.
11. Recover the message m using the formula m = cd mod n. The process will go back to the Schnorr algorithm.
12. Calculate x ≡ ar (mod p).
13. The receiver picks the password t.
14. This message is comprised of letters and spaces. The message t will go through the process of encryption using the RSA algorithm and the S-box and inverse S-box of the AES algorithm.
15. Convert each character to its two-digit number given in the table.

Blank	00	E	05	J	10	O	15	T	20	Y	25
A	01	F	06	K	11	P	16	U	21	Z	26
B	02	G	07	L	12	Q	17	V	22		
C	03	H	08	M	13	R	18	W	23		
D	04	I	09	N	14	S	19	X	24		

Fig. 5. Two-number digit representing each character.

16. Break the message into blocks of 2 letters containing four digits each.
17. Calculate ciphertext c using the formula c = me mod n. 18. Divide into blocks of 2 digits.
18. Convert to hexadecimal.
19. Encrypt the plaintext message using the Sbox to obtain the ciphertext. This is what the receiver sends to the sender.
20. The sender decrypts the ciphertext by converting it to decimal.
21. Convert to hexadecimal.
22. Apply the inverse S-box to obtain the original plaintext message.
23. Convert the original message to its decimal value.
24. Recover the message m using the formula m = cd mod n. m = t.
25. Divide into blocks of 2 digits and convert to its corresponding letter using the table in Figure 5. The process will go back to Schnorr algorithm.
26. The sender calculates y ≡ r +st (mod q) and sends it to the receiver.
27. The receiver tests verification is of authentication such that x′ ≡ ay • λt (mod p). The authentication will be accepted if x = x'.

Note:
The public keys are λ, n, and e.
The private keys are s and d.
The values of p, q, and φ(n) are private.

NUMERICAL STUDY ON THE HYBRID

1. Choose two distinct prime numbers, p and q, such that q (1 < q < p−1) is a prime factor of p−1.
p = 83
q = 41
(q = 41) is a prime factor of
(p-1) = (83-1) = 82
2. Choose a satisfying aq ≡ 1 (mod p).
a41 ≡ 1 mod 83
a41 – 1 = b / 83
341 ≡ 1 mod 83
a = 3
3. Choose s, such that s < q.
s = 36
(s = 36) < (q = 41)
4. Using the formula a•a-1 ≡ 1 mod p, calculate the multiplicative inverse of a.
3 (a-1) = 1 mod 83
3 (a-1) – 1 = 83
3 (a-1) = 83 +1
3 (a-1) = 84
a-1 = 28
5. Calculate λ ≡ a−s (mod p).
λ ≡ 2836 (mod 83)
λ ≡ 77
6. The sender selects r, such that r < q.
r = 25
(r = 25) < (q = 41)
r = m
7. Calculate n = p x q.
n = p x q = 83 × 41
n = 3403
8. Calculate φ(n) = (p-1) (q-1).
φ(n) = (p−1)(q −1) = 82 × 40
φ(n) = 3280
9. Select e, 1 < e < φ(n), such that e and φ(n) are coprime.
e = 53
gcd (53, 3280) = 1
10. Calculate d satisfying the congruence relation d ≡ e-1 mod φ(n).
d ≡ 53−1 (mod 3280)
d ≡ 557
a. Perform Euclidian Algorithm.
3280x + 53y = 1
3280 = 61 (53) + 47 equation 1
53 = 1 (47) +6 equation 2
47 = 7 (6) + 5 equation 3
6 = 1 (5) +1 equation 4
from equation 4
1 = 6 - 1 (5)
substitute (5) from equation 3
1 = 6 – 1 [47 – 7 (6)]
distribute
1 = 6 – 1 (47) + 7 (6)
combine similar terms
1 = 8 (6) – 1 (47)
substitute (6) from equation 2
1 = 8 [53 – 1 (47)] – 1 (47)
distribute
1 = 8 (53) – 8 (47) – 1 (47)
combine similar terms
1 = 8 (53) – 9 (47)
substitute (47) from equation 1
1 = 8 (53) – 9[3280 – 61 (53)]
distribute
1 = 8 (53) – 9 (3280) + 549 (53)
combine similar terms
1 = 557 (53) – 9 (3280)
Get the coefficient of y which is (53).
d = 557
b. Compute using extended Euclidian algorithm for verification.
ed ≡ 53 x 557 (mod 3280)
ed ≡ 29521 (mod 3280)
ed ≡ 1

11. Calculate ciphertext c using the formula c = me mod n.
c ≡ 2553 (mod 3403)
c ≡ 2751
12. Recover the message m using the formula m = cd mod n.

m ≡ 2751557 (mod 3403)
m ≡ 25

13. Calculate x ≡ ar (mod p).

x ≡ 325 (mod 83)
x ≡ 26

14. The receiver picks t. This will serve as the password for the authentication.

t = THE FIVE BOXING WIZARDS JUMP QUICKLY

15. Convert each character to its two-digit number given in the table in Figure 5.

T = 20, H = 08, E = 05, Blank= 00, F = 06,
I = 09,V = 22, E = 05, Blank = 00, B = 02,
O = 15, X = 24, I = 09, N = 14, G = 07,
Blank = 00, W = 23, I = 09, Z = 26, A = 01,
R =18, D = 04, S = 19, Blank = 00, J = 10,
U = 21. M = 13, P = 16, Blank = 00, Q = 17,
U = 21, I = 09, C = 03, K = 11, L = 12,
Y = 25

t=20080500060922050002152409140700230926011804190010211316001721090311122516. Break the message into blocks of 2 letters containing four digits each.

(T, H), (E, Blank), (F, I), (V, E),
(Blank, B), (O, X), (I, N), (G, Blank), (W, I), (Z, A),
(R, D), (S, Blank), (J, U), (M, P), (Blank, Q)
(U, I), (C, K), (L, Y)
m1 = (20 08), m2 = (05 00), m3 = (06 09),
m4 = (22 05), m5 = (00 02), m6 = (15 24),
m7 = (09 14), m8 = (07 00), m9 = (23 09),
m10 = (26 01), m11 = (18 04),
m12 = (19 00), m13 = (10 21),
m14 = (13 16), m15 = (00 17),
m16 = (21 09), m17 = (03 11),
m18 = (12 25)

17. Calculate ciphertext c using the formula c = me mod n.

c1 = 200853 mod 3403 = 204
c2 = 50053 mod 3403 = 718
c3 = 60953 mod 3403 = 2272
c4 = 220553 mod 3403 = 2533
c5 = 253 mod 3403 = 1714
c6 = 152453 mod 3403 = 2185
c7 = 91453 mod 3403 = 997
c8 = 70053 mod 3403 = 3277
c9 = 230953 mod 3403 = 954
c10 = 260153 mod 3403 = 1691
c11 = 180453 mod 3403 = 1353
c12 = 190053 mod 3403 = 683
c13 = 102153 mod 3403 = 510
c14 = 131653 mod 3403 = 1499
c15 = 1753 mod 3403 = 1211
c16 = 210953 mod 3403 = 1650
c17 = 31153 mod 3403 = 347
c18 = 122553 mod 3403 = 535

18. Divide into blocks of 2 digits.

(02 04), (07 18), (22 72),
(25 33), (17 14), (21 85),
(09 97), (32 77), (09 54),
(16 91), (13 53), (06 83),
(05 10), (14 99), (12 11),
(16 50), (03 47), (05 35)

19. Convert to hexadecimal.

(02 04), (07 12), (16 48),
(19 21), (11 0E), (11 55),
(09 61), (20 4D), (09 36),
(10 5B), (0D 35), (06 53),
(05 0A), (0E 63), (0C 0B),
(10 32), (03 2F), (05 23)

20. Encrypt the plaintext message using the S-box in Figure 2 to obtain the ciphertext. This is what the receiver sends to the sender.

(77 F2), (C5, C9), (47, 3B),
(D4 FD), (82 AB), (82 FC),
(01 EF), (B7 E3), (01 05),
(CA 39), (D7 96), (6F ED),
(6B 67), (AB FB), (FE 2B),
(CA 23), (7B 15), (6B 93)

21. Convert to decimal.

(119, 242), (197 201), (71 59), (212 253),
(130 171), (130 252), (01 239), (183 227),
(01 05), (202 57), (215 150), (111 237),
(101 103), (171 235), (254 43), (202 35),
(123 21), (107 147)

22. Convert to hexadecimal.

(77 F2), (C5, C9), (47, 3B),
(D4 FD), (82 AB), (82 FC),
(01 EF), (B7 E3), (01 05),
(CA 39), (D7 96), (6F ED),
(6B 67), (AB FB), (FE 2B),
(CA 23), (7B 15), (6B 93)

23. Apply the inverse S-box in Figure 3 to obtain the original plaintext message.

(02 04), (07 12), (16 48),
(19 21), (11 0E), (11 55),
(09 61), (20 4D), (09 36),
(10 5B), (0D 35), (06 53),
(05 0A), (0E 63), (0C 0B),
(10 32), (03 2F), (05 23)

24. Convert to decimal.

(02 04), (07 18), (22 72),
(25 33), (17 14), (21 85),
(09 97), (32 77), (09 54),
(16 91), (13 53), (06 83),
(05 10), (14 99), (12 11),
(16 50), (03 47), (05 35)

25. Recover the message m using the formula m = cd mod n. m = t.

m1 = 204557 mod 3403 = 2008
m2 = 718557 mod 3403 = 500
m3 = 2272557 mod 3403 = 609
m4 = 2533557 mod 3403 = 2205
m5 = 1714557 mod 3403 = 2
m6 = 2185557 mod 3403 = 1524
m7 = 997557 mod 3403 = 914
m8 = 3277557 mod 3403 = 3277
m9 = 954557 mod 3403 = 2309
m10 = 1691557 mod 3403 = 2601
m11 = 1353557 mod 3403 = 1804
m12 = 683557 mod 3403 = 1900
m13 = 510557 mod 3403 = 1021

m14 = 1499557 mod 3403 = 1316
m15 = 1211557 mod 3403 = 17
m16 = 1650557 mod 3403 = 2109
m17 = 347557 mod 3403 = 311
m18 = 535557 mod 3403 = 1225

26. Divide into blocks of 2 digits and convert to its corresponding letter given in the table in Figure 5.

T = 20, H = 08, E = 05, Blank= 00, F = 06,
I = 09, V = 22, E = 05, Blank = 00, B = 02,
O = 15, X = 24, I = 09, N = 14, G = 07,
Blank = 00, W = 23, I = 09, Z = 26, A = 01,
R =18, D = 04, S = 19, Blank = 00, J = 10,
U = 21. M = 13, P = 16, Blank = 00, Q = 17,
U = 21, I = 09, C = 03, K = 11, L = 12,
Y = 25

THE FIVE BOXING WIZARDS JUMP QUICKLY.

27. The sender calculates y ≡ r +st (mod q) and sends it to the receiver.

y1 = 25 + 36x2008 mod 41 = 30
y2 = 25 + 36x500 mod 41 = 26
y3 = 25 + 36x609 mod 41 = 14
y4 = 25 + 36x2205 mod 41 = 29
y5 = 25 + 36x2 mod 41 = 15
y6 = 25 + 36x1524 mod 41 = 31
y7 = 25 + 36x914 mod 41 = 6
y8 = 25 + 36x3277 mod 41 = 40
y9 = 25 + 36x2309 mod 41 = 1
y10 = 25 + 36x2601 mod 41 = 17
y11 = 25 + 36x1804 mod 41 = 25
y12 = 25 + 36x1900 mod 41 = 37
y13 = 25 + 36x1021 mod 41 = 4
y14 = 25 + 36x1316 mod 41 = 5
y15 = 25 + 36x17 mod 41 = 22
y16 = 25 + 36x2109 mod 41 = 17
y17 = 25 + 36x311 mod 41 = 28
y18 = 25 + 36x1225 mod 41 = 9

28. The receiver tests verification of authentication such that x′ ≡ ay • λt (mod p).

x"1 = 330 • 772008 mod 83 = 26
x"2 = 326 • 77500 mod 83 = 26
x"3 = 314 • 77609 mod 83 = 26
x"4 = 329 • 772205 mod 83 = 26
x"5 = 315 • 772 mod 83 = 26
x"6 = 331 • 771524 mod 83 = 26
x"7 = 36 • 77914 mod 83 = 26
x"8 = 340 • 773277 mod 83 = 26
x"9 = 31 • 772309 mod 83 = 26
x"10 = 317 • 772601 mod 83 = 26
x"11 = 325 • 771804 mod 83 = 26
x"12 = 337 • 771900 mod 83 = 26
x"13 = 34 • 771021 mod 83 = 26
x"14 = 35 • 771316 mod 83 = 26
x"15 = 322 • 7717 mod 83 = 26
x"16 = 317 • 772109 mod 83 = 26
x"17 = 328 • 7731 mod 83 = 26
x"18 = 39 • 771225 mod 83 = 26

Since x = x′, the authentication is accepted.

5 Conclusion

Encryption algorithm plays a very important role in communication security. This paper presents an effective method that combines techniques that can be used to successfully communicate and authenticate message in a secured manner. The proposed algorithm method provides a much-secured process of communication through the insertion of two cryptosystems in an authentication method. It lessens the effectiveness of interference of the attackers. It uses RSA algorithm which is one of the most effective and widely used cryptographic algorithms that withstood over three decades of assaults. It also uses the Rijndael S-box of AES algorithm which is considered to be the fastest algorithms in terms of the critical path between plaintext and the ciphertext. The addition of more steps through the insertion of these two cryptosystems to the algorithm reduces the probability of the success for the attackers.

References

[1] M. Preetha and M. NIthaya, "A Study and Performance Analysis of RSA Algorithm," Int. J. Comput. Sci. Mob. Comput., vol. 2, no. 2320–088X, pp. 126–139, 2013.

[2] L. Savu, "Schnorr Signcryption - Combining Public Key Encryption with Digital Signature," Kaspersky Acad., 2012.

[3] P. Katkade and G. M. Phade, "Application of AES algorithm for data security in serial communication," Proc. Int. Conf. Inven. Comput. Technol. ICICT 2016, vol. 2016, 2016.

[4] A. Elshobaky, M. Rasslan, and S. Guirguis, "Implementation of Schnorr Signcyption Algorithm on DSP," Int. J. Secur. Its Appl., vol. 9, no. 11, pp. 217–230, 2015.

[5] G. Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES, and AES) for Information Security," Int. J. Comput. Appl., vol. 67, no. 19, pp. 33–38.

[6] P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES, and RSA for Security," Globa; J. Comput. Sci. Technol. Network, Web Secur., vol. 13, no. 15 Version 1.0, pp. 15–22, 2013.

[7] M. Shankar and P. Akshaya, "Hybrid Cryptographic Technique Using RSA Algorithm and Scheduling Concepts," Int. J. Netw. Secure. Its Appl., vol. 6, no. 6, pp. 39–48, 2014.

[8] Arboleda ER. Secure and Fast Chaotic El Gamal Cryptosystem. Int J Eng Adv Technol. 2019;8(5):1693–9.

[9] Arboleda ER, Balaba JL, Espineli JCL. Chaotic Rivest-Shamir Adleman Algorithm with Data Encryption Standard Scheduling. Bull Electr Eng Informatics. 2017;6(3):219–27.

[10] Espalmado JMB, Arboleda ER. DARE Algorithm : A New Security Protocol by Integration of Different Cryptographic Techniques. Int J Electrical Comput Eng. 2017;7(2):1032–41.

[11] Downey, R.G., Griffiths, E.J.: Schnorr randomness. Electr. Notes Theor. Comput. Sci. **66**(1), 1199–1205 (2002)

[12] D. M. Freeman, "Schnorr Identification and Signature," < http://web.stanford.edu/class/cs259c/lectures/schnorr>, 2011. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1536414.1536440.

[13] M. Y. Rhee, "Internet Security: Cryptographic principles, algorithms, and protocols," John Wiley Sons Ltd, Atrium, South. Gate, Chichester, West Sussex PO19 8SQ, England, 2003, Br. Libr. Cat. Publ. Data, no. 0-470-85285–2, pp. 112, 119–120, 165–168, 179–181, 2003.

[14] S. Vinothini and Vasumathi, "A Study on RSA Algorithm for Cryptography," Int. J. Comput. Sci. Inf. Technol., vol. Vol. 5 (4), no. 0975–9646, pp. 5708–5709, 2014.

[15] A. Das, "Public-Key Cryptography: Theory and Practice, Mumbai," Pearson Educ. India, 2009.

[16] C. Nalini, Nagaraj, P. V. Anandmohan, D. V. Poornaiah, and V. D. Kulkarni, "An FPGA based performance analysis of pipelining and unrolling of AES algorithm," Proc. - 2006 14th Int. Conf. Adv. Comput. Commun. ADCOM 2006, pp. 477–482, 2006.

[17] M. Pitchaiah, D. Philemon, and Praveen, "Implementation of Advanced Encryption Standard Algorithm," Int. J. Sci. Eng. Res., vol. 3, no. 3, pp. 1048–1050.

[18] A. Hafsa, N. Alimi, A. Sghaier, M. Zeghid, and M. Machhout, "A Hardware-Software Co-designed AES-ECC Cryptosystem," no. 978, pp. 50–54, 2017.

[19] Abd-ElGhafar, A. Rohiem, A. Diaa, and F. Mohammed, Generation of AES Key Dependent S-Boxes using RC4 Algorithm," 13th Int. Conf. Aerosp. Sci. Aviat. Technol. Pap. ASAT-13-CE-24.

[20] D. Selent, "Advanced Encryption Standard," Rivier Acad. Journal, ISSN 1559-9388 (online version), vol. 6, pp. 1–14, 2010.

[21] Q. Zhang and A. Qunding, "Digital image encryption based on Advanced Encryption Standard(AES) algorithm," 5th Int. Conf. Instrum. Meas. Comput. Commun. Control. IMCCC 2015, pp. 1218–1221, 2015.

[22] Dellosa R, Fajardo A and Medina R. "A New Method of Location Estimation for Fingerprinting Localization Technique of Indoor Positioning System " ARPN Journal of Engineering and Applied Sciences 13 (48), 9427-9435