Applied cryptography in network systems security for cyberattack prevention

Applied Cryptography in Network Systems Security for Cyberattack Prevention

Abel Yeboah-Ofori[1]
School of Computing and Engineering
University of West London
London, UK
abel.yeboah-ofori@uwl.ac

Christian Kwame Agbodza[2]
Department of Education
University of Brighton
Brighton, UK
c.agbodza@brighton.ac.uk

Francisca Afua Opoku-Boateng[3]
Beacom College of Computer and Cyber Sc
Dakota State University
Madison, USA
francisca.opoku-boateng@dsu.edu

Iman Darvishi[1]
School of Computing and Engineering
University of West London
London, UK
21488578@student.uwl.ac.uk

Fatim Sbai[4]
School of Computing and Engineering
University of West London
London, UK
21480906@student.uwl.ac.uk

Abstract*-Application of cryptography and how various encryption algorithms methods are used to encrypt and decrypt data that traverse the network is relevant in securing information flows. Implementing cryptography in a secure network environment requires the application of secret keys, public keys, and hash functions to ensure data confidentiality, integrity, authentication, and non-repudiation. However, providing secure communications to prevent interception, interruption, modification, and fabrication on network systems has been challenging. Cyberattacks are deploying various methods and techniques to break into network systems to exploit digital signatures, VPNs, and others. Thus, it has become imperative to consider applying techniques to provide secure and trustworthy communication and computing using cryptography methods. The paper explores applied cryptography concepts in information and network systems security to prevent cyberattacks and improve secure communications. The contribution of the paper is threefold: First, we consider the various cyberattacks on the different cryptography algorithms in symmetric, asymmetric, and hashing functions. Secondly, we apply the various RSA methods on a network system environment to determine how the cyberattack could intercept, interrupt, modify, and fabricate information. Finally, we discuss the secure implementations methods and recommendations to improve security controls. Our results show that we could apply cryptography methods to identify vulnerabilities in the RSA algorithm in secure computing and communications networks.

Keywords: Applied Cryptography, Network Security, RSA, Interception, Interruption, Modification, Fabrication.

I. INTRODUCTION

The application of cryptography has been relevant in network security systems in securing information and communications in business-to-business, consumer-to-business, and consumer-to-consumer environments. Cryptography algorithms and different transposition systems have been used to secure data and networks in points of sales systems, including electronic commerce, chip-based payment systems, password, digital currency systems, and others [1], [2]. The objective of applied cryptography includes using a secret key, public key, and hash functions to ensure data confidentiality, data integrity, authentication, and non-repudiation in a secure network communication environment [1], [2]. Several cryptosystems such as Caesar Cipher, Vigenère Cipher, Rivest-Shamir-Adleman (RSA), EI Gamal, Diffie Hermann, DES, SDES and other encryption algorithms have been used to secure messages. The concepts consider plaintext encryption ciphertext decryption and plaintext [3]. The RSA security protocol such PGP for email security, SSL/TSL for web application, IPSec/IKE for IP data security, SILC for conference services security and SSH for terminal connection security with capabilities to support digital signatures [14]. However, providing secure communications channels in a network system to prevent interception, interruption, modification, and fabrication has become very challenging. Cyberattacks are deploying various methods and techniques to break into network systems to exploit digital signatures, VPNs, and others. Attackers deploy various passive and active attacks on the network systems. As a result, the threats and risks of interception, interruption, modification, and fabrication of information and communications traversing the network have increased exponentially. The passive attacker deploys reconnaissance and traffic analysis to stealthy observe the information flows, data structures, then duplicate or copy them, and sometimes use them in ID theft, intellectual property, and industrial espionage attacks. Further, in an active attack, the adversary uses brute force and other methods to penetrate the systems masquerade, and covertly tries to modify the systems, their contents, and sometimes causes replay and denial of service attacks, especially in a distributed environment. These penetrations could lead to data tampering, alteration, modifications, deletions, and diversions of delivery channels.

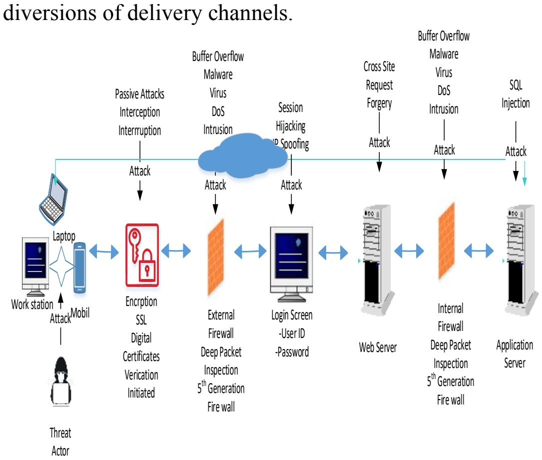

Fig 1. Network Attack

The objectives of applied cryptography focus on ensuring confidentiality, integrity, authentication, and non-repudiation of information and network systems. Thus, it has become imperative to provide a comprehensive study of how to apply cryptographic methods and techniques to provide secure and trustworthy communication and

978-1-6654-7878-6/21/$31.00 ©2021 IEEE
DOI 10.1109/ICSIoT55070.2021.00017

computing. The paper explores applied cryptography concepts in information and network systems security to prevent cyberattacks and improve secure communications. The contribution of the paper is threefold: First, we consider the various cyberattacks on the different cryptography algorithms in symmetric, asymmetric, and hashing functions. Secondly, we apply the various methods on a network system environment to determine how information could be intercepted, interrupted, modified, and fabricated by the cyberattack. Finally, we discuss the secure implementations methods and provide recommendations to improve security controls. Our results show that applied cryptography methods could be used to identify vulnerabilities in secure computing and communications networks.

II. RELATED WORKS

This section provides an overview of the start of the art and related works in applied cryptography and network systems security. Applied cryptography considers various symmetric, asymmetric and algorithms methods and hashing functions to transform and transpose data in a secure format from senders and receivers. For instance, Jana et al. (2021) analyzed elliptic curve cryptography in network security. The authors proposed some statistical results by using a small key size compared to RSA and Diffie Hermann algorithms to reduce processing overhead [4]. Devi (2013) explored the applications of network security and cryptographic algorithms on information security by discussing the implications of digital signatures in RSA and how various attacks are deployed on it [5]. Further, Huang et al. (2007) proposed a generic transformation algorithm that converted any unforgeable signatures scheme into strongly unforgeable ones and kept the key pair of the signature schemes unchanged. They used a strong one-time signature scheme based on a one-way function, relevant in a trapdoor hash function [6]. Additionally, Huang et al. (2014) proposed a partial key exposure attack on Takagi's variants of the RSA algorithm by considering the Coppersmith method to find the small roots of the modular polynomial equations. The authors use three key scenarios: the most significant bits, the least significant bits, and the middle bits of the private exponent, respectively, on RSA of Ernst et al., partial key exposure attacks [3]. Lu et al. (2014) proposed a new partial key exposure attack on CTR-RSA with large public exponents by introducing two approaches using lattice-based attacks for the extended settings [7]. Yoneyama et al. 2014, proposed a password-based authentication Key exchange scheme without a centralized trust setup by focusing on a multi-string model that allows several authorities to provide some reference strings independently [8]. Zhang et al. (2014) proposed an all-but-one dual project hashing and its applications by providing a simple construction of all but one lossy trapdoor function and constructing a chosen-text-attack secure determination encryption scheme in a standard model [9]. Finally, Keifer and Manulis (2014) explored using a two-server password authentication key exchange application by proposing an extended distributed smooth projective hash function. The authors used the Cramer-Shoup cyphertexts method to compute distributed hash values across several parties to authenticate key exchange protocols [10]. Bakhatiari and Maarof (2012) posits that RSA cryptosystems have serious weakness in its implementation. The authors demonstrated a method to encrypt and decrypt the RSA algorithm by indicating that the number factorization method in a serious threat against RSA [14]. However, RSA remains the most difficult to attack and exploit if user secure the algorithm properly during implementation in commercial cryptosystems.

A. Security Objectives

We briefly discuss security objectives in applied cryptography, including data confidentiality, data integrity, authentication, and non-repudiation in a secure network communication environment [8] [11].

B. Data Confidentiality

Data confidentiality considers preserving authorized restrictions on access and disclosure to information. The objective is to protect and preserve personal privacy and proprietary data in information sharing and network platforms. For instance, the attacker could deploy a passive attack to covertly carry out reconnaissance, traffic analysis, penetrations, intellectual property theft, industrial espionage, and command and control attacks [8] [11].

C. Data integrity

Data integrity considers securing the network against improper information modification or destruction. For instance, an attacker could deploy an active attack after penetration and intercept, modify and fabricate data that could lead to information non-repudiation and authenticity. In addition, other attacks such as brute force, distributed denial of service, and ransomware attacks could deploy, leading to other cascading impacts on the information and network systems [8] [11].

D. Data Authentication

Data Authentications consider trusting the sources of the information and proper attribution to the owner or creator of the data. In business process and information sharing, it ensures that a system or person's authorizations, policies, statements, and permissions issues are genuine. For instance, an attacker could exploit digital signatures when data authenticity is not enforced. Further, the attacker would be violating the authenticity of an altered e-mail message sent that appear to have come from a different e-mail address than the source [8] [11].

E. Non-Repudiation

Non-repudiation provides the assurance that an object or a system cannot deny a previous commitment or action. It indicates that some data sources cannot deny that this is the case to a third party. It is a most desirable property in transactions where there is the potential for a dispute to arise over the exchange of information [8], [11].

All the works contribute to applied cryptography and network security. However, none of the works considered applied cryptography and encryption algorithm from interception, interruption, modification, and fabrications from an information and network security perspective.

III. APPROACH

The proposed approach considers the RSA cryptosystem model within the network security systems domain. We use the algorithm to determine how attacks are deployed on the encryption algorithms to cause interception, interruption, modification, and fabrication attacks to data using RSA encryption and decryption methods [4] [5]. The strength of the encryption used is dependent on the cryptographic algorithm and the number of decryption keys. We explain the cryptography algorithms briefly as follows.

A. Cryptographic Algorithms

Cryptographic algorithms could be considered from different classifications methods and categorized based on the key lengths used for the encryption and decryptions. We categorize Cryptographic algorithms into three methods: symmetric, asymmetric, and hashing functions [1], [12]. We discuss the concepts briefly as follows using Figure 2.

A. Symmetric Encryption

Symmetric encryption is a private key cryptosystem in which encryption and decryption are done in a conventional manner using the same key. The encryption transforms plaintext into ciphertext using a secret key and an encryption algorithm. Then using the same key and a decryption algorithm, the plaintext is recovered from the ciphertext. Symmetric encryption is susceptible to brute force attacks as it uses transposition techniques [12].

B. Asymmetric Encryption

Asymmetric encryption uses a public key cryptosystem to encrypt a message with one key and decrypt with another key using pairs of keys for the public and private. The key generation system relies on cryptographic algorithms and uses a one-way function based on the mathematical method [12]. For instance, in a cryptosystem, the RSA algorithm is computationally infeasible to determine the decryption key when given only the knowledge of the cryptographic algorithm and then the encryption key [12].

C. Hashing Functions

Hashing functions are used as a cryptographic algorithm to map random size data to a fixed-size value hash [12]. The hash values are used to determine the integrity of data storage and information retrievals. In addition, the hash functions are used for checksums and error correction codes for data optimization.

D. Interception, Interruption, Modification, and Fabrication Attacks

The goal of applied cryptography in information and network systems security is to ensure security mechanisms are implemented to prevent interception, interruption, modification, and fabrication of data with the objectives of enforcing confidentiality, integrity, authenticity, and non-repudiation [8], [11]. In a network system, the attacker penetrates a network system using interception, interruption, modification, and fabrication attacks to exploit victims [13]. We discuss the methods briefly as follows.

a. Interception Attack

Allow unauthorized users to access data, applications, or environments, and are primarily an attack against confidentiality. Interception might take the form of unauthorized file viewing or copying, eavesdropping on phone conversations, or reading e-mail, and can be deployed against data at rest or in motion. Properly executed, interception attacks can be challenging to detect.

b. Interruption Attack

The attacker diverts the communications flows to another source to prevent the authorised user from accessing the information. Thus, causing information and assets to become unusable or unavailable to use, either temporarily or permanently. This attack affects availability and data integrity. For instance, a DDoS attack on a mail server could be classified as an availability attack. In addition, the attacker could manipulate the database processes which a database runs to prevent access to data. That could lead to an integrity attack and possible loss or corruption of data or both.

c. Modification Attack:

Involves tampering, altering, and modifying data after the attacker has interrupted the information flows, business processes, or delivery channels. These attacks lead to integrity violations as it causes the data to be unavailable to legitimate users. For instance, accessing a file in an unauthorized manner and altering the data affects the integrity of the data contained in the file. A configuration file acting as a Web server that manages how a service performs might be affected by the availability and integrity of that service by changing the file's contents. Altering the Web server file configuration further affects how the server deals with encrypted connections, leading to confidentiality and privacy attacks. A modification attack on a database server is considered an interruption attack.

d. Fabrication Attack

Involves generating false data, processes, communications, or other similar activities within a system to fabricate the legitimate user after modifying the contents. The primary objective of fabrication attacks is to generate false information in a database that primarily affects the integrity and availability attack. For instance, the attacker could modify and falsify an e-mail after interrupting and forward it to the recipient in a spoofing attack, propagating malware attacks. Further, the attacker could cause DDoS attacks and an availability attack by generating enough additional processes, network traffic, e-mail, web traffic to consume resources and render the service that handles such traffic unavailable to system users.

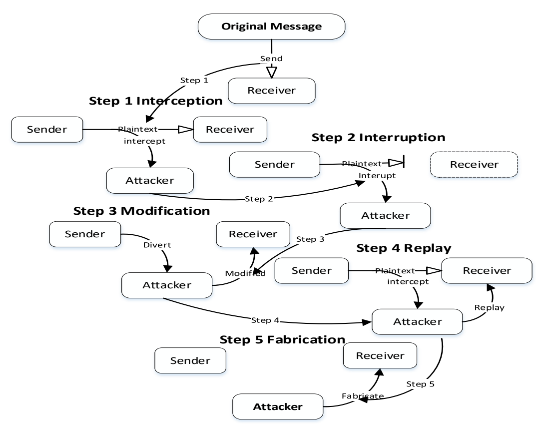

Fig. 2. Interception Interruption Modification Fabrication Attacks Method

IV. IMPLEMENTATION

V. This section considers the RSA cryptographic implementation method discussed in section 3 and how the attacker deploys interception, interruption, and modification. Fabrication attacks methods on the network system [3], [7], [11], [13] using a modular arithmetic method.

A. The RSA Cryptosystems Deployment Steps

1. Plaintext: The original message or data that will be inputted into the algorithm.
2. Encryption algorithm: The algorithm performs various transpositions and transforms the plaintext ciphertext.
3. Public and private keys: Pairs of keys selected for encryption or decryption depending on input and transformation algorithm.
4. Ciphertext: The plaintext that is scrambled and generated as output depending on the plaintext and the key.
5. Decryption algorithm: The algorithm decrypts the ciphertext and produces a matching key for the original plaintext message generated as output for the recipient

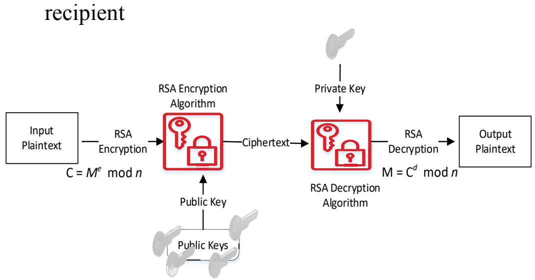

Fig. 3. RSA Public Key Cryptosystem

Attack Steps:

1. Pairs of Keys are generated for each user's message encryption and decryption
2. A public key will be placed in a public register for accessibility, and the private key is kept by each user and maintains a set of public keys acquired from others.
3. If a sender wants to send a private message to a receiver, the sender encrypts the receiver's message using the public key.
4. When the receiver gets the message, it decrypts it using the private key, known only by the receiver.

B. The RSA Algorithm

The RSA algorithm method used for encryption and decryption comprises of Public and Private (p, q) keys: The setup randomly chooses large primes p; q as n = p,q, where *n* is the number of primes. The greatest common divisor (gcd) is used to determine the encrypted message. We used the modular arithmetic formula to encrypt and decrypt the message in transition as follows:

- Message = M
- Key = k
- Encryption = *e*
- Ciphertext = C
- Decryption = D
- Public Key = p

Private key = q
Modular = mod

We choose a number *e* such that gcd (e; (p - 1)(q - 1)) = 1

$$\text{find } d \equiv e^{-1} \bmod (p-1)(q-1) \qquad (1)$$

Public key = (n; e), private key = (p; q; d)

Encryption:

$$C = M^e \bmod n$$

Decryption:

$$M = C^d \bmod n$$

A source *A* produces a message *X* intended for *B* in as,

$$X = \{X_1, X_2, \ldots, X_n\} \qquad (2)$$

The *M* elements of *X* are letters in some finite alphabet. Thus, B generates a related pair of public key PU_b and private key PR_P.

Source *A* form a ciphertext with a message *X* and the encryption key PU_b using the algorithm

$$Y = [Y_1, Y_2, \ldots, Y_n] \qquad (3)$$
$$Y = E(PU_b, X)$$

The recipient in possession of the private key can invert the transposition using the algorithm:

$$X = E(PR_b, Y) \qquad (4)$$

C. Encryption

Sender *A* wants to send a message to *B* with msg M = 10.
A key value k is chosen randomly. For instance, k = 3
Sender A calculated C_1 :

$$C_1 \equiv g^k \bmod p \qquad (5)$$
$$\equiv 11^3 \bmod 23$$
$$\equiv 20 \bmod 23$$

To complete the encryption, the sender must calculate C_2:

$$C_2 \equiv M \times y^k \bmod p \qquad (6)$$
$$\equiv 10 \times 9^3 \bmod 23$$
$$\equiv 22 \bmod 23$$

D. Decryption

Receiver B receives the ciphertext (20; 23) (7)
The receiver starts by finding $D \equiv C_1^x \bmod p$

$$D \equiv 20^6 \bmod 23$$
$$\equiv 16 \bmod 23$$

Further, the receiver calculates $D^{-1} \bmod p$:

$$D^{-1} \equiv 16^{-1} \bmod 23 \qquad (8)$$
$$\equiv 13 \bmod 23$$

Finally, the receiver recovers message M:

$$M \equiv C_2 \times D^{-1} \bmod p \qquad (9)$$
$$\equiv 22 \times 13 \bmod 23$$
$$\equiv 10 \bmod 23$$

E. RSA Encryption and Decryption Using OpenSSL Tool

The purpose of the RSA implementation is to encrypt and decrypt using Public and private keys in using SSL command in Mac operating system terminal in a network environment. The tool used for our RSA implementation is the Open SSL for encryption and decryption. We explain the implementation process and steps as follows:
Step1: Create RSA Private Key default 2048 bit using OpenSSL:

```
OpenSSL> genrsa -out private.pem
Generating RSA private key, 2048 bit long modulus
.....+++
.................+++
e is 65537 (0x10001)
OpenSSL>
```

Figure 4. Generating SSL using Privat Key

Step 2: Figure 4 explains how we create a file for the key with a size of 4096 bit for the length of the size using OpenSSL to make the private key *(Pr)* more secure by typing the command: "genrsa -our private.pem 4096"

```
OpenSSL> genrsa -out private.pem 4096
Generating RSA private key, 4096 bit long modulus
...........................++
........................++
e is 65537 (0x10001)
OpenSSL>
```

Fig 5. Create a File for Key Size Length

Step 3: Figure We create a public key using RSA algorithm with the key based on the private key created in step 2 (*Pu*) we have created:

```
OpenSSL> rsa -pubout -in private.pem -out public.pem
writing RSA key
OpenSSL>
```

Fig 6. Public Key Output

Step 4: To view the encrypted file content of our public key that we use, and to view the text in private.pem we use the command: OpenSSL rsa -text -in private.pem

Figure 7displays the private key and public key contents and the key component in plain text. The addition encoded version is used to encode with the key data but we can find both of them here

```
Imans-iMac:~ imandarvishi$ cat public.pem
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAr0FcLZ+4P1l7xfAVktUq
LTTTD3YH4HAAjENOE/6WVKRru4d7gBbViA0GH74UUlUZt1GjneYsp0MMIbhjp000
oP3bnv2llBZmd39ebqQ1ZOvO35iPANAKyK6T1s6wkgQeHKDche4KypV8IsDUb8Fj
1xItj8r0tM8pAKFd1sdzZ7wHnT50KHsBWCsi3c657xr1Bnu9D9tNiQSyD197OUly
u0MConL0eKqsBd+dijBq24yMAGH+PT6a1LClPxddcbYRMEQBXwYLdLZ0L1rHQiC5
HE7yEPJdvsdjBFLtnJSSq7Ed2NogwpubfmJQI8cM3GRpxX+OxZ8p09z/15gKS+NC
4QkBxs1fhrboPE5BYrGdfY3upXFyADoIZBVXjZ/XEqh5QbJCz6LZPPtMnBNwPFft
lk7sHUWgLxtVGv/AZJ0TmlG1y33Nnqlm2HpA7qzQ01dwDcY4k3e/ZV2p5+YwePMy
6GZaS/3jk2x4tUKkg2ShTutKKmUz3xfhk09lpdWSYnBofM2WyXt51v/gRdA1Sca6
unZDFQsAue7czlOzsAhpjYWVDQWsvvxsQF4wLqD2iwqSD7AHY4nmpYPR8j3mVAvW
nwc++KbtNjAoyv+fBct2VAYhN5KjrE2uj4CZ6BTHwUlNwAY5t1OjwBakPXF5cRLO
ftbTtzcM89T3VpHxK4MiW1UCAwEAAQ==
-----END PUBLIC KEY-----
Imans-iMac:~ imandarvishi$
```

Fig 7. Public Key

Step 5: In Figure 7, we created a file and encrypted it using the public key in step 4 to decrypt the file later. We typed the command: Vim hello.txt

The command allows us to create a new file to use for encryption and decryption.

We type "Hello" in the file content as our message for us to be able to encrypt.

Now to encrypt the "hello.txt" file using the public key and put the output into a new file called demo_encrypt.txt: by using the command:

Openssl rsautl -encrypt -in hello.txt -pubin -inkey public.pem -out demo_encrypt.txt

Step 6: Now to view the content of the hello.text file into the demo_encrypt.txt file, we used the command: xxd demo_encrypt.txt.

The figure provides us with a large key since we used a key size of 4096 bits for the length of the encryption and decryption, as discussed in step 2.

```
Imans-iMac:~ imandarvishi$ cat public.pem
-----BEGIN PUBLIC KEY-----
Imans-iMac:Desktop imandarvishi$ xxd demo_encrypt.txt
00000000: bad9 d77e e60e 13de 3bb8 d0c2 8a85 19c0  ...~....;.......
00000010: 0f4d 8229 767c 2182 229f 8290 a5d0 a797  .M.)v|!.".......
00000020: 542f 106e 849d ba16 7c21 9e99 abba 28ae  T/.n....|!....(.
00000030: 641d 2f4a 00c4 c745 eebb 28a9 a343 32f3  d./J...E..(..C2.
00000040: 2362 47a4 07a2 a103 2248 9619 6c01 b319  #bG....."H..l...
00000050: 7c58 bf66 d22f 1317 8a7d 2635 fa46 b328  |X.f./...}&5.F.(
00000060: 1f9a 1ca1 3ead 735f f1da d3d2 ea71 312e  ....>.s_.....q1.
00000070: dd28 8e95 886e d034 06f5 9eaa 4eef a945  .(...n.4....N..E
00000080: 1370 36da b63b 5fff 9853 1221 2fc9 39fc  .p6..;_..S.!/.9.
00000090: 959e 05cb 318b 85ea 4958 21dd 49bf 6649  ....1...IX!.I.fI
000000a0: 178b e0ea e3d3 0f47 2b43 0f63 742b 3d8f  .......G+C.ct+=.
000000b0: 3304 868f 3c32 b6cc bfa3 9337 fbaa 39fd  3...<2.....7..9.
000000c0: 4789 4ad8 3e56 fa4f 5acf 9e33 bf98 0e92  G.J.>V.OZ..3....
000000d0: 3afa a307 bb2e 39f5 604a 8077 04b8 bfc1  :.....9.`J.w....
000000e0: b414 d05c e6e9 1e98 dd02 e5d0 7b55 a421  ...\........{U.!
000000f0: 32ab 31c5 b4e2 1a14 53db 6396 9a33 87c4  2.1.....S.c..3..
00000100: fb6f a079 6f86 26eb 969d ec34 2ee5 c75e  .o.yo.&....4...^
00000110: d985 6aa9 7399 b580 1118 b6ef c4ee 16b9  ..j.s...........
00000120: 4e3b 0711 a63b ac78 b8e1 5ad7 133e c025  N;...;.x..Z..>.%
00000130: d85d 26fd e272 6b43 49ed aae6 eb60 80d6  .]&..rkCI....`..
00000140: 8412 2d8a eb5a 5eb0 2c0d 3727 db2b 6cf4  ..-..Z^.,.7'.+l.
00000150: 74a1 9e38 f7c1 57b5 776d d3c6 c8ff 1494  t..8..W.wm......
00000160: 8f21 d84a cc46 dd77 2902 c772 476e 68bd  .!.J:F.w)..rGnh.
00000170: 1d61 c845 cf2a 9e94 a498 0e44 0931 29a6  .a.E.*.....D.1).
00000180: 8c0b 2f8b 91d0 85cd cb7d c47d 3216 8c77  ../......}.}2..w
00000190: 273a 119a fa35 1f2e ab96 0101 e703 471d  ':...5........G.
000001a0: 06ae 01f4 a736 04ce e503 38ef 7f3d 20d4  .....6....8..= .
000001b0: fc3b 8b44 f9b0 1896 955e cbc9 1fa2 c000  .;.D.....^......
000001c0: 23b6 79bc 2406 1542 7592 f849 ec63 da9d  #.y.$..Bu..I.c..
000001d0: 493c 406f 2c6e 4851 9f8a 92ee 213a b563  I<@o,nHQ....!:.c
000001e0: c18d 7b89 2e9b a376 e533 f984 b57b 98ee  ..{....v.3...{..
000001f0: 3cf4 bff7 3191 c790 e44c 4d8e 5811 0c39  <...1....LM.X..9
```

Fig 8. Output of Cyphertext

Step 7: To Decrypt the file "demo_encrypt.txt" that contains the message "hello" from a decrypted version into a plaintext, We used the same private key we created in step 2 into a new file name called demo_decrypt.txt: e used this command:

Openssl rsautl -decrypt -in demo_encrypt.txt -inkey private.pem -out demo_decrypt.txt

Step 8: Finally, we have decrypted our file to the original message as in Figure 9. To view the file the content, we use the following command:

Cat demo_decrypt.txt

```
Imans-iMac:Desktop imandarvishi$ xxd demo_decrypt.txt
00000000: 6865 6c6c 6f0d                           hello.
Imans-iMac:Desktop imandarvishi$
```

Fig 9. Decrypted Text

F. Results

The results show that by using the OpenSSL tool, we generated a private RSA key with a custom length of 4096, then we made a public key using the same RSA key, the public key contains the key length plus the encoded details. Further, we created one file containing our sender message we have encrypted the file using the public key and finally we decrypted the file with its private key. Considering we are encrypting using asymmetric, we must have the private key to be able to decrypt the encrypted message.

Several cryptosystems and other encryption algorithms have been used to secure messages such as RSA, EI Gamal, Diffie Hermann, DES, SDES. However, RSA is suitable for businesses and online payment transactions in a symmetric key encryption. In addition, RSA is faster to encrypt, uses fewer resources, uses block cyphers, uses asymmetric keys and is more secure.

VI. DISCUSSIONS

A. Adversarial Attack on Data Confidentiality

The adversary's goal is to cause an attack on data confidentiality by intercepting and interrupting network and information flows to deny information preservation and authorized restrictions to access and disclosure. For example, the adversary can intercept message *A* by targeting and observing Y and having access to PU_b but having access to PR_b or X attempts to recover X and PR_b using the algorithm. In an instant where the adversary's only motive is to intercept the message, then the focus is to recover message X by generating a plaintext estimate at $n=X$. The adversary knows the algorithm encryption key (E) and decryption (D).

In an instant where the adversary wants to Interrupt the message and modify it, the adversary recovers the PR_b by generating the algorithms that attempt to modify the message. These attacks impact data protection and preservation of personal privacy and proprietary data on network systems information-sharing platforms.

B. Adversarial Attack on Data Authentication

The adversary's goal is to cause an attack on data authentication and deny trust in information integrity where permissions are issues by a system or a person. An adversary attacks a transmission source *A* where a private key is used to prepare a message and send to source *B* to decrypt using the public key from *A*. For instance, a message that serves as a digital signature could be altered when the attacker gets access to the private key owned by *A* during transmission. Thus, compromising the authenticity and integrity of the source and contents of the message from *B,* as data could be modified after being intercepted and fabricated.

C. Security Factors to Consider when choosing Cryptographic Mechanisms

Due to varying organizational security requirements, different factors are considered when choosing cryptographic mechanisms. For instance, an organization security mechanism may consider the appropriateness of the cryptosystem, security strength, and cost of implementation. Appropriateness to Organizational Goal: consider factors that determine cryptographic tools required for the organization goal. The appropriateness of the tools determines the importance and specific properties that a cryptographic mechanism will provide to ensure security and information assurance.

Security Strength: considers the type of security requirements and cryptographic mechanism for a particular network system. Different data security mechanisms are required for different levels of information protection.

Cost Benefit and Return on Investment considers the security gains and financial worth

Does that justify the costs of securing the systems and the information that traverses the network? An organization may measure the cost of security in terms of ease of use of encryption algorithm and its efficiency for the business operation. Security operations and applications considerations use cost as a determinant of their adopted security mechanisms instead of the strength of the cryptosystem of the security that the encryption mechanism provides.

VII. CONCLUSION

Applying cryptography methods, encryption techniques, and algorithms to provide secure and trustworthy network communications and information security has been challenging. The paper has discussed the various attack methods such as interception, interruption modification, and fabrication that adversaries deploy to compromise network systems and information flows. Further, we have discussed how the RSA public-key cryptosystem can be compromised and how adversaries could attack the network systems and data encryption algorithms during transmission to corrupt the information's confidentiality, integrity, and authenticity. Finally, the paper has shown how to identify vulnerabilities and apply cryptography methods to prevent cyberattacks on network communication systems.

Future works will consider information and network security using Homomorphic encryptions in a Cyber-physical systems environment.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practices.* 2014.

[2] M. Leno, *Cryptography Applications: What Is The Basic Principle Of Cryptography?: Cryptography Number Theory.* 2020.

[3] Z. Huang, L. Hu, J. Xu, L. Peng, and Y. Xie, "Partial Key Exposure Attacks on Takagi's Variant of RSA," in *Applied Cryptography and Network Security*, vol. 8479, I. Boureanu, P. Owesarski, and S. Vaudenay, Eds. Cham: Springer International Publishing, 2014, pp. 134–150. doi: 10.1007/978-3-319-07536-5_9.

[4] B. Jana and J. Poray, "A performance analysis on elliptic curve cryptography in network security," in *2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE)*, Kolkata, India, Dec. 2016, pp. 1–7. doi: 10.1109/ICCECE.2016.8009587.

[5] T. R. Devi, "Importance of Cryptography in Network Security," in *2013 International Conference on Communication Systems and Network Technologies*, Gwalior, Apr. 2013, pp. 462–467. doi: 10.1109/CSNT.2013.102.

[6] Q. Huang, D. S. Wong, and Y. Zhao, "Generic Transformation to Strongly Unforgeable Signatures," in *Applied Cryptography and Network Security*, vol. 4521, J. Katz and M. Yung, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 1–17. doi: 10.1007/978-3-540-72738-5_1.

[7] Y. Lu, R. Zhang, and D. Lin, "New Partial Key Exposure Attacks on CRT-RSA with Large Public Exponents," in *Applied Cryptography and Network Security*, vol. 8479, I. Boureanu, P. Owesarski, and S. Vaudenay, Eds. Cham: Springer International Publishing, 2014, pp. 151–162. doi: 10.1007/978-3-319-07536-5_10.

[8] K. Yoneyama, "Password-Based Authenticated Key Exchange without Centralized Trusted Setup," in *Applied Cryptography and Network Security*, vol. 8479, I. Boureanu, P. Owesarski, and S. Vaudenay, Eds. Cham: Springer International Publishing, 2014, pp. 19–36. doi: 10.1007/978-3-319-07536-5_2.

[9] Z. Zhang, Y. Chen, S. S. M. Chow, G. Hanaoka, Z. Cao, and Y. Zhao, "All-but-One Dual Projective Hashing and Its Applications," in *Applied Cryptography and Network Security*, vol. 8479, I. Boureanu, P. Owesarski, and S. Vaudenay, Eds. Cham: Springer International Publishing, 2014, pp. 181–198. doi: 10.1007/978-3-319-07536-5_12.

[10] F. Kiefer and M. Manulis, "Blind Password Registration for Two-Server Password Authenticated Key Exchange and Secret Sharing Protocols," in *Information Security*, vol. 9866, M. Bishop and A. C. A. Nascimento, Eds. Cham: Springer International Publishing, 2016, pp. 95–114. doi: 10.1007/978-3-319-45871-7_7.

[11] W. Stallings, *Cryptography and Network Security: Principles and Practice.* 2020.

[12] M. Jhuria, S. Singh, and R. Nigoti, "A Survey of Cryptographic Algorithms for Cloud Computing," *Int. J. Emerg. Technol. Comput. Appl. Sci.*, May 2013.

[13] Engineering Libretext, "1.4 Attacks - Types of Attacks," *Engineering LibreTexts*, Jan. 11, 2021. https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks (accessed Sep. 12, 2021).

[14] M. Bakhtiari and M. A. Mararof, "Serious Security Weakness in RSA Cryptosystem" IJCSI International Journal of Computer Science Issues, Semantic Scholar, 2012. Vol. 9, Issue 1, No 3,