ASH1925015M

by Iftekhar Efat

Submission date: 13-Mar-2022 01:21AM (UTC-0500)
Submission ID: 1782984875
File name: ASH1925015M.pdf (431.94K)
Word count: 1781
Character count: 9314

Effects of RSA on network security

Shahriar Ahmed
ASH1925015M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security ....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

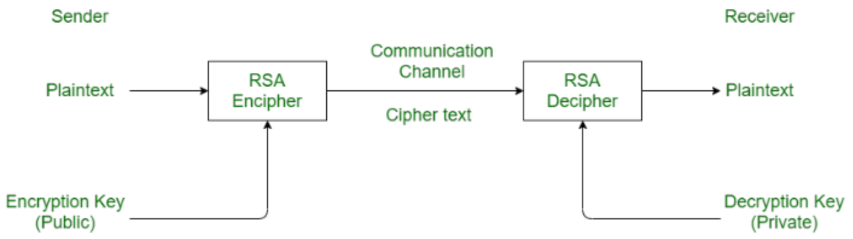
OPTIONAL: I give permission this work to be reproduced and provided to future students as an exemplar report.

Abstract

Information Security has become an essential concern in the modern world.Encryption is an effective way to prevent an unofficial person from viewing the digital information with the secret key. RSA encryption is often used for digital signatures which can prove the authenticity and reliability of a message. As RSA encryption is less competent and resource-heavy, it is not used to encrypt the entire message. If a message is encrypted with a symmetric-key RSA encryption it will be more efficient. Under this process, only the RSA private key will be able to decrypt the symmetric key. The proposed algorithm shows its better performance in terms of speed, throughput, power consumption, and the avalanche effect. Experimental results and mathematical justification supporting the proposed method are reported.

1 Introduction

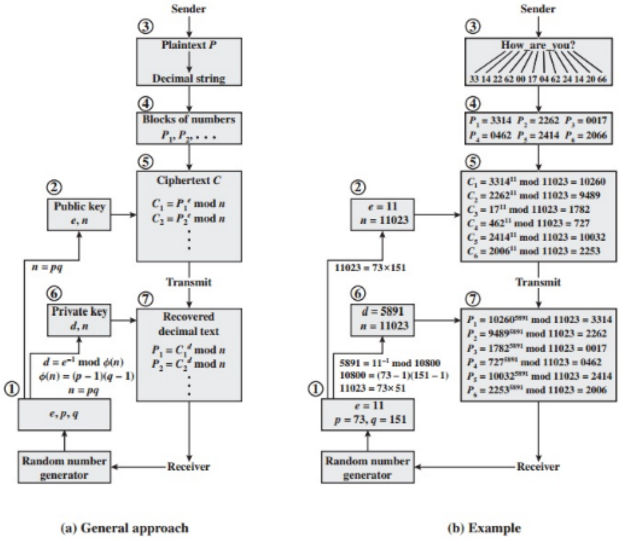
RSA is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric cryptographic algorithm. RSA operations can be decomposed in three broad steps; key generation, encryption and decryption. The arithmetic used in RSA for encrypting and decrypting is known as modular arithmetic. The RSA algorithm security is a function of the difficulty involve in factorizing n to obtain p and q prime numbers. To obtain n is easy i.e. by multiplying p and q but to obtain the prime numbers p and q which is the reverse operation of factorizing n is practically impossible especially when p and q are large numbers. RSA key size should modulus up to 2048 bits as suggested by several organizations (Lenstra and Verheul 2001). The keys size that RSA typically uses is 1024 to 2048. The RSA standard is in specified RFC 3447, RSA Cryptography Specifications Version 2.1 . In RSA cryptography, both the public and private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This quality is one reason why RSA has become the most extensively used asymmetric algorithm. It provides a method to declare the confidentiality, integrity, authenticity, and non-repudiation of electronic communications and data storage.The RSA algorithm is the base of a cryptosystem a set of cryptographic algorithms that are used for explicit safety services or resolve which allows public-key encryption and is broadly used to safeguard the data, mainly when in actuality it is directed over an insecure network such as the internet.



2 Key Generation Procedure

There are some steps for generating key. [5]
1. Choose two distinct large random prime numbers p q such that p q.
2. Compute n= p × q.
3. Calculate: phi (n) = (p-1) (q-1).
4. Choose an integer e such that 1¡e¡phi(n)
5. Compute d to satisfy the congruence relation d × e = 1 mod phi (n); d is kept as private key exponent.
6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

Encryption Plaintext: P ¡ n Ciphertext: C= Pe mod n.
Decryption Ciphertext: C Plaintext: P=Cd mod n


Sender
③
Plaintext P
Decimal string
④
Blocks of numbers
$P_1, P_2, \ldots$
⑤
Ciphertext C
$C_1 = P_1^e \bmod n$
$C_2 = P_2^e \bmod n$
②
Public key
e, n
$n = pq$
Transmit
⑥
Private key
d, n
⑦
Recovered decimal text
$P_1 = C_1^d \bmod n$
$P_2 = C_2^d \bmod n$
$d = e^{-1} \bmod \phi(n)$
$\phi(n) = (p-1)(q-1)$
$n = pq$
①
e, p, q
Random number generator
Receiver
Sender
③
How_are_you?
33 14 22 62 00 17 04 62 24 14 20 66
④
$P_1 = 3314$ $P_2 = 2262$ $P_3 = 0017$
$P_4 = 0462$ $P_5 = 2414$ $P_6 = 2066$
⑤
$C_1 = 3314^{11} \bmod 11023 = 10260$
$C_2 = 2262^{11} \bmod 11023 = 9489$
$C_3 = 17^{11} \bmod 11023 = 1782$
$C_4 = 462^{11} \bmod 11023 = 727$
$C_5 = 2414^{11} \bmod 11023 = 10032$
$C_6 = 2006^{11} \bmod 11023 = 2253$
②
$e = 11$
$n = 11023$
$11023 = 73 \times 151$
Transmit
⑥
$d = 5891$
$n = 11023$
⑦
$P_1 = 10260^{5891} \bmod 11023 = 3314$
$P_2 = 9489^{5891} \bmod 11023 = 2262$
$P_3 = 1782^{5891} \bmod 11023 = 0017$
$P_4 = 727^{5891} \bmod 11023 = 0462$
$P_5 = 10032^{5891} \bmod 11023 = 2414$
$P_6 = 2253^{5891} \bmod 11023 = 2006$
$5891 = 11^{-1} \bmod 10800$
$10800 = (73-1)(151-1)$
$11023 = 73 \times 51$
①
$e = 11$
$p = 73, q = 151$
Random number generator
Receiver

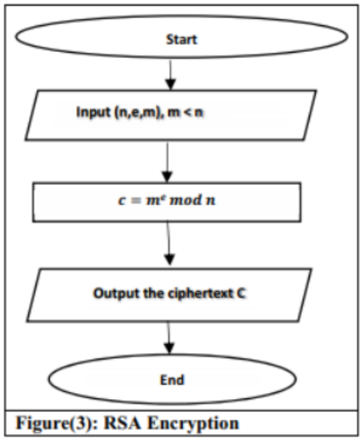
(a) General approach

(b) Example

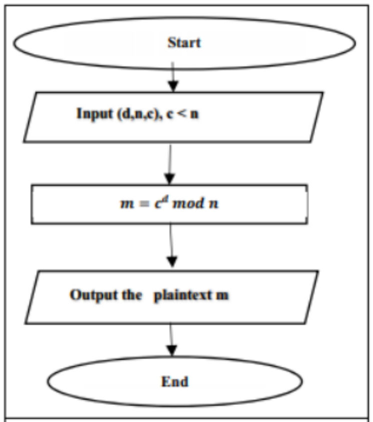
Figure 9.7 RSA Processeing of Multiple Blocks

3 RSA Security

RSA security [3] is from factorization of problem. Difficulty of The RSA security is a function of how large is the number to be factorized. It ensure fast factorization algorithms are used like Trial division, Pollard's rho, Pollard's p-1, Quadratic sieve, elliptic curve factorization, Random square factoring and Number field sieve among others. Also, RSA is commonly used in electronic commerce protocols, and is believed to be safe given adequately long keys and the utilization of up-to-date implementations (Borodzhieva and Manoilov 2008).



Figure(3): RSA Encryption

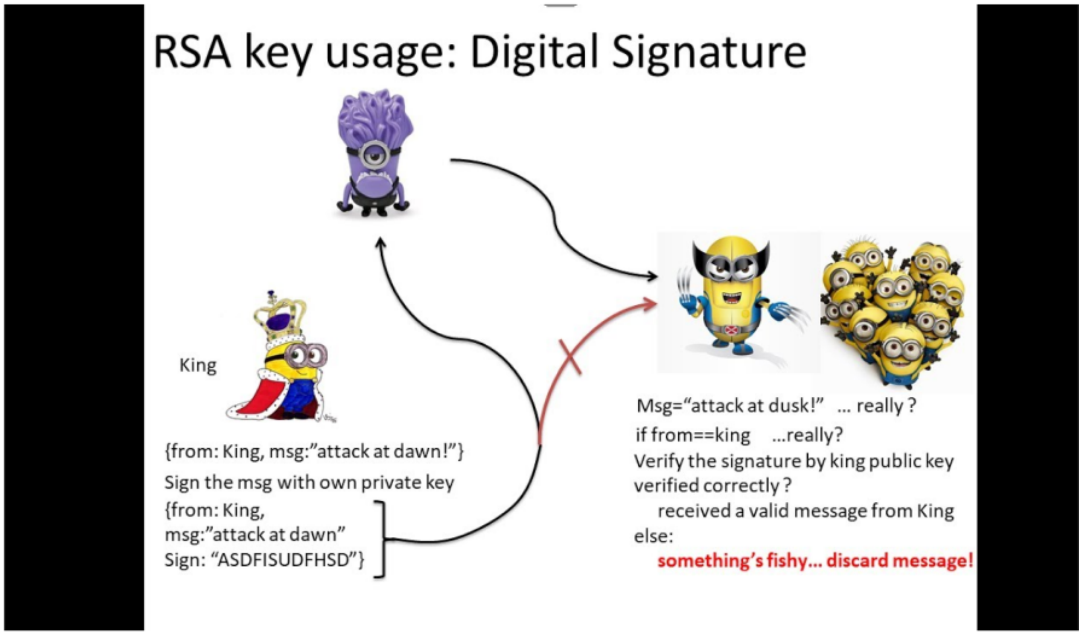


Figure(4): RSA Decryption

RSA attacks [4] can be categorized into four categories and they are:
(1) Elementary attacks that exploit blatant misuse of the system
(2) Low private exponent attacks serious enough that a low private exponent should never be used
(3) Low public exponent attacks
(4) And attacks on the implementation (Boneh 1999).

4 RSA Usage

RSA is widely used in many protocols that are security oriented. These security oriented protocols are outlined as follows : [4] 1. Transport Layer Security (TLS) and Secure Sockets Layer (SSL) - transport data security (web)
2. Pretty Good Privacy (PGP) - email security
3. Secure Shell (SSH) - terminal connection security
4. Secure Internet Live Conferencing (SILC) - conferencing service security among other.



RSA key usage: Digital Signature

{from: King, msg:"attack at dawn!"}
Sign the msg with own private key
{from: King,
msg:"attack at dawn"
Sign: "ASDFISUDFHSD"}

Msg="attack at dusk!" ... really ?
if from==king ...really?
Verify the signature by king public key
verified correctly ?
received a valid message from King
else:
something's fishy... discard message!

5 Limitation of RSA Algorithm

The problem with RSA algorithm [2] is slow decryption process due to increase or doubling of key length.
1.The use of small p and q is also a limitation because small key length is insecure i.e. an eavesdropper could recover the plaintext.
2.Another limitation is the encryption speed which can be overcome using a protocol known as the digital envelope.
3.RSA algorithm limitation that could occur in the near future is design of TWIRL (The Weizmann Institute Relation Locator) which is a hypothetical hardware device that can speed up the sieving step of the general number field sieve integer factorization algorithm.

6 RSA Techniques Today

The RSA cryptography [1] is the widely use public key cryptography in the world today. It is the crypto system deployed in thousands of applications today round the world to maintain security. Thus, there have being several records of RSA systems compromised. Moreover, it is still most widely used public key cryptography. This is because standards have been put in place to ensure RSA cryptography survival. Since complicated systems are sometime liable to compromise, there is the need for there to be standards. These standards when follow regularly ensure better and more secure systems. The RSA standards are regularly updated by RSA cryptography professionals worldwide to regularly update RSA crypto system. PKCS 1 version 2.1 is the newest standard used by RSA crypto system today. There exist widely accepted standards for most cryptographic operations, such as the Advanced Encryption Standard (AES) for secret-key encryption and 2048- bit RSA for public-key encryption. These primitives have been widely studied, and hacking them is believed to be computationally impossible on any existing computer cluster (Bernstein et al 2012). Today, SSL Secure Sockets Layer uses 2048 bit encryption to establish secure connection with other application, web browsers and email programs. The secure SSL notify online customers about unsecure application. RSA is extensively used in electronic commerce protocols, and is believed to be safe given adequately long keys and the use of up-to-date implementations (LOKULWAR et al 2012). RSA cryptography is still a suitable security measure for electronic data. Thus, the weakness of the algorithm is due to the used of low private exponent. Low private exponent should never be used because there have been records of low public key attacks ranging from brute force attack, subtle attack among other. RSA cryptography must be correctly employed to avoid attack (Singh et al 2012). Table 2 below shows RSA key lengths that were recommended to protect lifetime of confidential data (Shamir Tromer's estimate, Kaliski (2003)).

7 Effects of RSA

When we use RSA algorithm in our network security system,it prevents various attacks from the attackers.It is because an attacker can't guess the two primary key.That's why it is quite impossible to break network security. It is used for the security purpose in the wide range of networks.

8 Conclusions

The advent of computer networks and internet has made it possible to send and receive information with ease. Computer hackers on the other hand have been threats to this technology. Over the years, these threats lead to computer and internet security to prevent malicious users from gaining access to vital information. This thesis examines supply chain security, supply chain information security and the use of RSA techniques. The RSA technique is a secured standard for public key cryptography. It helps to secure supply chain information. The thesis also shows that supply chain security is very important in supply chain management. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used.The use of 2048 bits or more RSA techniques are better for high security protection due to difficulties involve in factorizing large prime numbers. It could be infer that, 2048 bits or more bits are recommended for better supply chain security. Moreover, further studies should be carried out on RSA techniques on supply chain security.

References

[1] Behrad Garmany and Tilo Müller. Prime: Private rsa infrastructure for memoryless encryption. In *Proceedings of the 29th Annual Computer Security Applications Conference*, pages 149–158, 2013.

[2] Mays M Hoobi, Sumaya S Sulaiman, and Inas Ali AbdulMunem. Enhanced multistage rsa encryption model. In *IOP Conference Series: Materials Science and Engineering*, volume 928, page 032068. IOP Publishing, 2020.

[3] Priyadarshini Patil, Prashant Narayankar, DG Narayan, and S Md Meena. A comprehensive evaluation of cryptographic algorithms: Des, 3des, aes, rsa and blowfish. *Procedia Computer Science*, 78:617–624, 2016.

[4] KR Raghunandan, Rovita Robert Dsouza, N Rakshith, Surendra Shetty, and Ganesh Aithal. Analysis of an enhanced dual rsa algorithm using pell's equation to hide public key exponent and a fake modulus to avoid factorization attack. In *Advances in Artificial Intelligence and Data Engineering*, pages 809–823. Springer, 2021.

[5] Gurpreet Singh. A study of encryption algorithms (rsa, des, 3des and aes) for information security. *International Journal of Computer Applications*, 67(19), 2013.

ASH1925015M

ORIGINALITY REPORT

88%	89%	17%	61%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	publications.theseus.fi Internet Source	55%
2	turcomat.org Internet Source	8%
3	Submitted to Kingston University Student Paper	6%
4	Submitted to University of Lancaster Student Paper	6%
5	v1.overleaf.com Internet Source	5%
6	research.ijcaonline.org Internet Source	4%
7	global.oup.com Internet Source	2%
8	Submitted to Stourbridge College Student Paper	2%
9	www.coursehero.com Internet Source	1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925015M

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

Confused You have used **its** in this sentence. You may need to use **it's** instead.

PAGE 3

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

Missing "," You may need to place a comma after this word.

Missing "," You may need to place a comma after this word.

PAGE 4

PAGE 5

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to remove this article.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Possessive This word may be a plural noun and may not need an apostrophe.

Article Error You may need to use an article before this word.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

PAGE 6

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

PAGE 7

Article Error You may need to use an article before this word. Consider using the article **a**.

Article Error You may need to use an article before this word.

PAGE 8

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

PAGE 9

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to remove this article.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.