Network Security Encryption techniques for reliablility data transmission on password system

Ng Liang Shen , Norrozila Sulaiman, Mohamed Ariff Ameeden

[1] Universiti Malaysia Pahang, Gambang, 26600, Malaysia

Abstract. The desire to transmit messages securely is not new. For centuries, community kept communication in secret. Nowadays, with the latest technology particularly the internet, vast amount of data transmit sensitive information but able to intercept easily if it is not encrypted before sending to the intended recipient. Encryption and decryption algorithm for secure communication depends on the algorithm while the internal structures of the robustness of the mathematics computation depend on the key it uses. A ciphertext can be transmitted openly across a communications channel. Because of its encrypted nature, eavesdroppers who may have access to the ciphertext will ideally be unable to uncover the message meaning. Only the intended recipient can decrypt the message to recover the plaintext for interpretation. An improved RSA algorithm using dynamic key from the private key from the receiver is proposed by dictating which key length to act according to bit length of an acceptable level key length for encryption and different lengths for complex algorithm, which increases the computing speed and increase the degree of security.

Keywords RSA; Private Key; Public Key; Key Length; Optimization;

1 Introduction

With the implementation of the internet, sudden surge in usage of about 90% of the entire community communicated through email. Thus increase the important of secure data integrity in public environment [1]. In some systems, one-way functions are used for logging onto a network or application program to protect the secrecy during transmission medium [2]. However the Hash functions take the input (password) and convert it into an output string from which the input string cannot be determined. The receiving party does not need to know the input string corresponding to an output string in a received message. Therefore while sending to unsecure channel, only the hash password is sent but until now, the effectiveness for changing password has not been proven [3]. Lately, various encryption broadcasts medium offer high security and efficiency but the key algorithms product of plaintext length consume processing speed to encrypt the message and the transmission rate is low when decrypting by the receiver. At this moment there is no effective solution [3].

At present, RSA has been applied for decade and it is often the desired security parameter [4]. RSA is one of the most popular cryptography systems that received detailed attention in research area as well as commercial domain. Many authors have studied it weaknesses and identify the flaws. Currently there is application such as Wireshark which is able to sniff the password easily. By using RSA, is there any way to prevent this from happening [5]. In this paper, a new algorithm for reconstructing RSA variable private keys length is presented. The RSA' algorithm applicability is derived from algorithm properties like: confidentiality, safe authentication, data safety and integrity in public network [7].

While establishing new RSA variable key length, problems may arise regarding the authentication level and also the authorization for the authenticate person. Many of the security problems are solved but still some attacks are not yet been countermeasure, and new attacks are taking birth on daily basis may be on hourly basis [8].

2 RSA Algorithms

Static Key Length = 8 bit Public Key Pair (E, N) Private Key Pair (D, N)

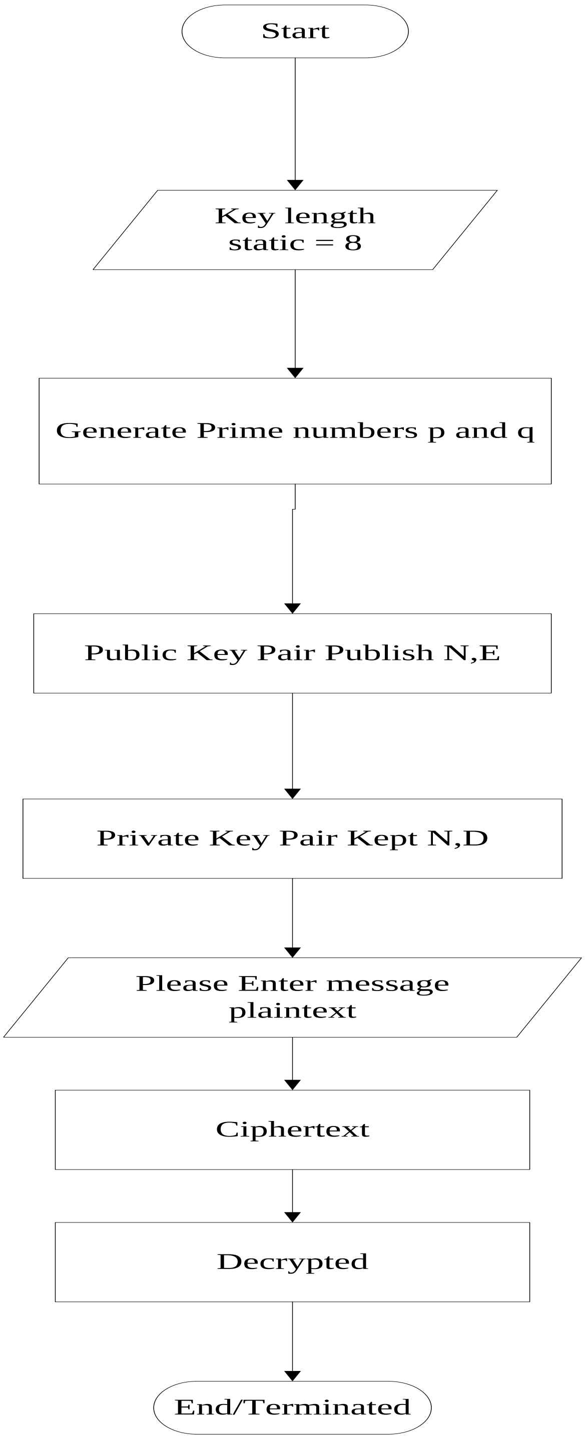
Start
Key length static = 8
Generate Prime numbers p and q
Public Key Pair Publish N,E
Private Key Pair Kept N,D
Please Enter message plaintext
Ciphertext
Decrypted
End/Terminated

Figure 2.1 Flowchart of RSA Algorithms

One predicament which we discovered with RSA Algorithm is that was it uses a static private key thus increase the vulnerability which might be discovered , With the implementation a dynamic or variable key private key Length N module must be greater than any other key of the client key. It thus makes the encryption key length more complexity. to improve the variable length key for the private key and to enhance new possibilities for the algorithm exploration further. The previous RSA Algorithm use times to determine the greatest common divisor of two positive integers. The key length of the variable Key Length is around 8 bit to 2048 bit [6][7].

Dynamic Key Length = 8 bit to 2048 bit [8]

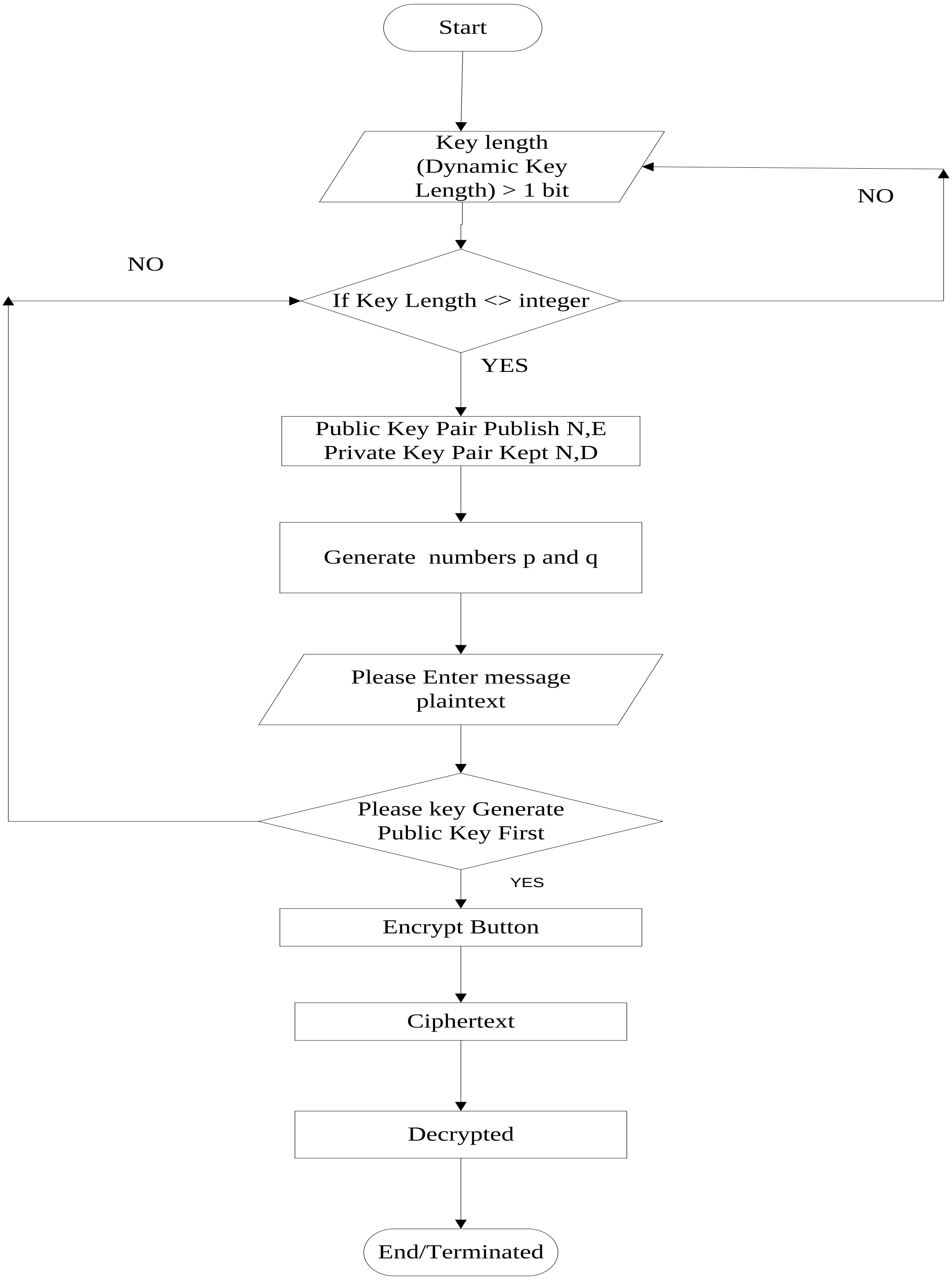
Start
Key length (Dynamic Key Length) > 1 bit
NO
NO
If Key Length <> integer
YES
Public Key Pair Publish N,E
Private Key Pair Kept N,D
Generate numbers p and q
Please Enter message plaintext
Please key Generate Public Key First
YES
Encrypt Button
Ciphertext
Decrypted
End/Terminated

Fig. 1: The Improved RSA Algorithms

3 Results

The improved RSA Algorithms is using private Key Length bit Algorithms by increasing the complexity of the nature in order to avoid been sniffed. The diagram below is to show how easy traffic been captured by sniffing tools like Wireshark, by displaying the optimization speed [2]. Even the optimization is 3 seconds different, for 8 bit it is 19 second and 16 bit is 24 second.

```
Enter key size: Key Size: [8]

Generated prime numbers p and q
p: [9D]
q: [89]
The public key is the pair (N, E) which will be published.
N: [5405]
E: [524B]
The private key is the pair (N, D) which will be kept private.
N: [5405]
D: [A03]

Please enter message (plaintext):
Universiti Malaysia Pahang
Ciphertext: [FE 43CC 133C 37C1 32CC 4844 3C6B 133C E14 133C DF2 2E45 53D0 2BB2 53D0
1424 3C6B 133C 53D0 DF2 302D 53D0 1490 53D0 43CC 34D5]

Recovered plaintext: [Universiti Malaysia Pahang]
BUILD SUCCESSFUL (total time: 19 seconds)
```

Variable Key Length

```
Enter key size:  16
Key Size: [16]
Generated prime numbers p and q
p: [F2BF]
q: [C03B]
The public key is the pair (N, E) which will be published.
N: [B6473205]
E: [35EF7041]
The private key is the pair (N, D) which will be kept private.
N: [B6473205]
D: [2D547021]

Please enter message (plaintext):
Universiti Malaysia Pahang
Ciphertext: [6B95E49F 68EA8578 28B384F 89AFFB74 783321CE 5BCC8240 23B69F8B
28B384F B2F4FD3 28B384F 63D6AC8F 6D0AE618 1C557D4C 62107797 1C557D4C
B234DE51 23B69F8B 28B384F 1C557D4C 63D6AC8F 863048FB 1C557D4C 620B866

F 1C557D4C 68EA8578 831F69AE]
Recovered plaintext: [Universiti Malaysia Pahang]
BUILD SUCCESSFUL (total time: 24 seconds)
```

4 Conclusion

In conclusion, has highlighted the issue in RSA algorithm and an improved algorithm using dynamic key from the private key was proposed to improve date security.

5 References

[1] Eskicioglu, Ahmed M, 2001, IEEE, Cryptography, pages 36 – 38.

[2] Xin,Zhou, and Xiaofei Tang, August 22-24, 2011, Research and Implementation of RSA Algorithm for Encryption and Decryption, The 6th International Forum on Strategic Technology, page 1118 - 1121.

[3] Peyravian, Mohammad and Zunic Nevenko, 2000, Methods for Protecting Password Transmission, Elsevier, pages 466 – 469.

[4] Mao,Jane and Zhang Jianhong, 2011, An efficient RSA-based certificateless Signature scheme, Elsevier, pages 638-642.

[5] Sakar, Santanu, Maitra, Subhamoy, 2010, Cryptanalysis of RSA with more than one decryption exponent, Elsevier, pages 336 – 340.

[6] Mircea Frunza', Luminita Scripcariu, 2007,IEEE, Improved RSA Encryption Algorithm for Increased Security of Wireless Networks, Pages 4244-0969.

[7] Nadia Heninger, Hovav Shacham,2007, Improved RSA Private Key Reconstruction for Cold Boot Attacks,pages 1-17

[8] Masood Habib, Tahir Mehmood, Fasee Ullah, Muhammad Ibrahim, 2009, International Conference on Computer Technology and Development, Performance of WiMAX Security Algorithm, (The Comparative study of RSA Encryption Algorithm with ECC Encryption Algorithm), pages 1-5.