Email Encryption Using Hybrid Cryptosystem Based on Android

Saranzaya Purevjav*, TaeYang Kim**, HoonJae Lee**

*Department of Ubiquitous IT, Graduate School of Dongseo University, Sasang-gu, Busan 617-716, Korea

** Division of Information and Engineering, Graduate School of Dongseo University, Sasang-Gu, Busan 617-716, Korea

saranzaya @gmail.com, hjlee@dongseo.ac.kr

***Abstract*—21st century is often called the Information Century. Information technology is being used in all areas of life from medicine to astronomy. The list of developments and advances happened in those areas thanks to information technology penetration is endless. As the world become digitized more and more and information technology becomes ubiquitous, creating electronic and digital phenomena such as digital economy, e-democracy, e-government, e-business, e-bank, e-health system, e-education, even e-agriculture, traditional illegal activities are penetrating into the virtual world as well. As a result, an entirely new type of criminal activities has emerged threatening the security and integrity of the system, network, and information. In case of a system error, it can be fixed after a certain amount of time, but how about information security? This is becoming one of the most important problems. There is classified information that can have implications on national level. Even the best encryption and highest security firewalls can be breached to delete, steal, or change such protected information. Therefore, we need implementing hybrid cryptosystem. This paper focus on securing e-mail communication on Android OS by using the hybrid cryptosystem which is a combination of symmetric, public key encryption system and hash function.**

***Keywords*— Hybrid cryptography, symmetric encryption, secure email, public key encryption**

I. INTRODUCTION

Most popular internet services is e-mail. Email is way to exchange text by using internet connection. Now almost internet services can be enjoyed by using mobile devices such as notebook, smartphone and tablet PC anywhere and anytime. Purposely, or not, the usage of e-mail to exchange information and collaborate, is not only limited to public information, but also confidential information, which has a value of confidentiality to certain parties so that it needs some security controls. By using mobile devices with internet connection, e-mail services can be widely used by many people to exchange information and collaborate, both for individual, enterprise and government. One of the most popular Operating System is Android. In order to prove safety of email sent from Android smart phone, encryption and decryption process have to be installed in an client side. All security systems use cryptographic because it suggest several algorithms and techniques practically unavailable to break because of their entanglement. In this proposed design methodology, the new protocol design using Symmetric cipher (Ping Pong-128) and public key cryptography (RSA) with hash function MD5.

II. BACKGROUND

What is the need of hybrid cryptosystem?

Cause of:

- Conventional encryption system uses one key.
- If key is disclosed then complete encryption vulnerable.
- Key distribution problem.
- To provide greater security and avoid explicit transfer of secret key we need hybrid cryptosystem.

Public key and symmetric ciphers each have their own advantages and disadvantages. The public key algorithms allow public key infrastructures and key exchange systems, but at the cost of speed. Symmetric ciphers are significantly faster than public key encryption, but require all parties to somehow share a secret key. A hybrid cryptosystem is a protocol using multiple ciphers of different types together, each to it is best advantage. Hybrid cryptosystem is considered as highly secure type of encryption as long as the public and private keys are fully secure.

A. Symmetric cryptography

This kind of cryptography uses a single key for both encryption and decryption, and it is also called secret key cryptography. The key is a set of rules, and both the sender and the receiver must know the key in order to use the technique. The most known secret key cryptography schemes are stream ciphers and block ciphers[1]. The stream ciphers generate a sequence of bits used as a key called a keystream, and the encryption is accomplished by combining the keystream with the plaintext. This is usually done with the bitwise XOR operation. The keystream can be independent of the plaintext and cipher text, in which case the stream cipher is synchronous, or it can depend of the data and its encryption, in which case the stream cipher is self-synchronizing[2].

B. Asymmetric cryptography

The public key cryptographic algorithms are more secure than symmetric algorithms. Because, it has two keys one for

encryption and another one for decryption. In this hybrid encryption technique we propose symmetric encryption for encryption and decryption and using public key cryptosystems for authentication [3].

C. Hash Function

A hash function offers a way of creating a fixed-size blocks of data by using entry data with variable length. It is also known as taking the digital fingerprint of the data, and the exit data are known as message digest or one-way encryption. . The hash values solve the problem of the integrity of the messages.

III. HYBRID CRYPTOSYSTEM SCHEME

Symmetric and asymmetric ciphers each have their own advantages and disadvantages. Symmetric ciphers are significantly faster than asymmetric ciphers, but require all parties to somehow share a secret (the key). The asymmetric algorithms allow public key infrastructures and key exchange systems, but at the cost of speed. A hybrid cryptosystem is a protocol using multiple ciphers of different types together, each to it is best advantage [4]. In order to implement aspects of information security in the e-mail communication system, it will use the mechanism of the hybrid cryptosystem which combines symmetric encryption, asymmetric encryption and hash function. The cryptographic algorithms consist of Ping Pong 128 bit encryption for confidentiality, MD5 bit for data integrity, while aspects of authentication and non-repudiation use a combination of MD5 bit and RSA 1024 bit.

This crypto security system ensures:

- Data integrity- using hash function
- Authentication and authenticity – using digital signature
- Data confidentiality – using stream cipher (Ping Pong)

A. Ping Pong

The advantage of a stream cipher is that it is faster and much more efficient than block ciphers. PingPong family of stream ciphers. It has two mutually clocking LFSRs and a single memory bit. The LFSRs are of lengths 127 bits and 129 bits. Together with the memory bit they give PingPong-128 an internal state of 257 bits. PingPong-128 takes a 128-bit key and a 128-bit initialisation vector to fill the internal state. Keystream Generation The PingPong generator produces the output keystream by combining the LFSR sequences and the memory sequence [5]. PingPong-128 has two mutually clocking LFSRs L_a and L_b, and a single bit of memory c. Two primitive polynomials, Pa(x) and Pb(x) are following:

$$P_a(x)=x^{127}\oplus x^{109}\oplus x^{91}\oplus x^{84}\oplus x^{73}\oplus x^{6}\oplus x^{66}\oplus x^{63}\oplus x^{56}\oplus x^{55}\oplus x^{52}\oplus x^{48}\oplus x^{45}\oplus x^{42}\oplus x^{41}\oplus x^{37}\oplus x^{34}\oplus x^{30}\oplus x^{27}\oplus x^{23}\oplus x^{21}\oplus x^{20}\oplus x^{19}\oplus x^{16}\oplus x^{13}\oplus x^{12}\oplus x^{7}\oplus x^{6}\oplus x^{2}\oplus x^{1}\oplus 1$$

$$P_b(x)=x^{129}\oplus x^{125}\oplus x^{121}\oplus x^{117}\oplus x^{113}\oplus x^{109}\oplus x^{105}\oplus x^{101}\oplus x^{97}\oplus x^{93}\oplus x^{89}\oplus x^{85}\oplus x^{81}\oplus x^{77}\oplus x^{73}\oplus x^{69}\oplus x^{65}\oplus x^{61}\oplus x^{57}\oplus x^{49}\oplus x^{45}\oplus x^{41}\oplus x^{37}\oplus x^{33}\oplus x^{29}\oplus x^{25}\oplus x^{21}\oplus x^{17}\oplus x^{13}\oplus x^{9}\oplus x^{5}\oplus 1$$

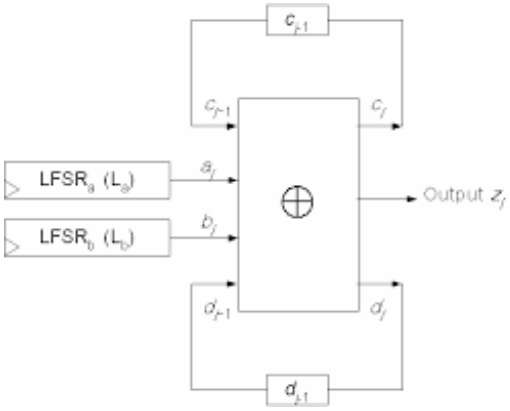

Figure 1. Ping Pong – 128 Generator

B. RSA

The security of RSA is generally considered to factoring. RSA computation occurs with integers modulo n = p * q, for select two random secret primes p, q. To encrypt a message m, public key use a public key exponent e. so cipher text c = me (mod n) computes the multiplicative reverse d = e-1 (mod (p-1)*(q-1)) (we require that e is selected suitably for it to exist) and obtains cd = m e * d = m (mod n)[4]. The problem for the attacker is that computing the reverse d of e is assumed to be no easier than factorizing n. The key size should be greater than 1024 bits for a reasonable level of security. Keys of size, say, 2048 bits that provides.

Digital signatures employ asymmetric cryptography. In many instances they provide a layer of validation and security to messages sent through insecure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender. To create RSA signature keys, generate an RSA key pair containing a modulus N that is the product of two large primes, along with integers e and d such that $e\,d \equiv 1 \pmod{\varphi(N)}$, where φ is the Euler phi-function. The signer's public key consists of N and e, and the signer's secret key contains d.

To sign a message m, the signer computes $\sigma \equiv m^d \pmod N$. To verify, the receiver checks that $\sigma^e \equiv m \pmod N$.

As noted earlier, this basic scheme is not very secure. To prevent attacks, one can first apply a cryptographic hash function to the message m and then apply the RSA algorithm described above to the result[6].

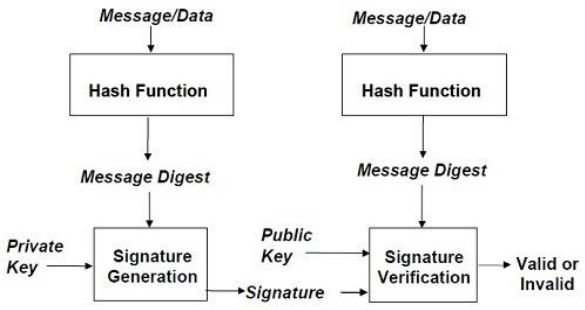

Figure 2. Digital Signature

C. *Proposed Architecture*

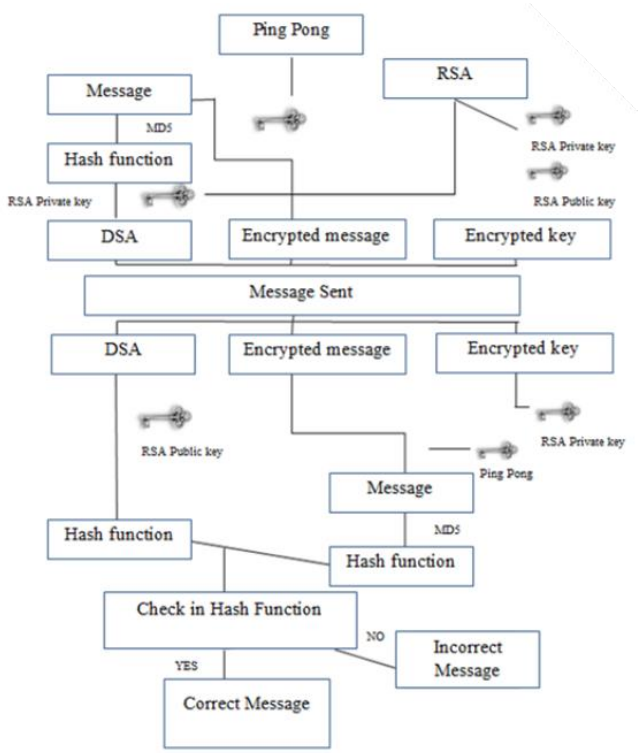

Figure 3. Hybrid Cryptographic scheme for Email

D. *Experiment*

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

```
Run:
-------GENRATE PUBLIC and PRIVATE KEY------------
Public Key - Sun RSA public key, 2048 bits
  modulus:
161675758773944989882617900630782324338359936895539800223103739O
520015325199507513909368224591430650537224533875405996172931067S
114636428930772747538834283303395032315455913878629455895508032820
891600160454048127159412055288955734037755884452502201405425333B3
818960879000139123743268032142379644041909197779824246700507412A4
942238008922493236144504557707316235151286956746424673207872O331
752690340898058590698780129459386681222433337441299297004916188Z0
026514920406286284538003365591215442036344773813903051765424973G
377494852004147894487567094186504595151373497282765802346074416Y
940788751507678879613854704383985133668O39
  public exponent: 65537
Private Key - sun.security.rsa.RSAPrivateCrtKeyImpl$Ffe98f55

--------SAVING PUBLIC KEY AND PRIVATE KEY TO FILES-------

Generating Public.key...
Public.key generated successfully
Generating Private.key...
Private.key generated successfully

----------------ENCRYPTION STARTED------------
Data Before Encryption :This is RSA encryption created by CNSL
Encryted Data: [B@1c6b6478
----------------ENCRYPTION COMPLETED------------

----------------DECRYPTION STARTED------------
Decrypted Data: This is RSA encryption created by CNSL !
----------------DECRYPTION COMPLETED------------
BUILD SUCCESSFUL (total time: 6 seconds)
```

Figure 4. RSA key generation

Digesting a String with MD5 can be done with the MessageDigest class. We can get a MessageDigest object that can be used to do an MD5 digest via Message.Digest.getInstance ("MD5"). We can pass the MessageDigest a byte array representation of the String that we'd like to digest. Calling the digest() method on the MessageDigest object will return a byte array representation of the MD5 digest. It's very common to convert this to its Hex representation.

```
original:secret
digested(hex):5ebe2294ecd0e0f08eab7690d2a6ee69
```

Figure 5. Hash Function generation

IV. CONCLUSIONS

We know that E-Technology usage is increasing day by day. Most of us use smart phone, tablet and computer all day long without realizing it. So, we will need realize to encryption for application of smart phone/Android OS/. Hybrid encryption is a mode of encryption that merges two or more encryption systems. These strengths are respectively defined as speed and security. Therefore, we are suggest design of hybrid cryptographic for secure email based on Android OS.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (Grant number: NRF-2011-0023076). And it also supported by the BB21 project of Busan Metropolitan City.

REFERENCES

[1] William Stallings (2003), Cryptography and Network Security-Principles and Practices, 3rd Edition, Pearson Education Asia

[2] Menezes AJ, Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. Florida: CRC PressInc. 1996.

[3] Ramaraj E, Karthikeyan S, Hemalatha M. A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA). International Journal of The Computer, the Internet and Management. 2009; 17(1):78-86

[4] Prof. Patrick McDaniel, Network and Security Research Center Department of Computer Science and Engineering Pennsylvania State University, University Park PA – "Public-Key Cryptography and Attacks on RSA", 2010

[5] Prof. HoonJae Lee, Kevin Chen, 2007 International Conference on Convergence Information Technology "PingPong-128, A New Stream Cipher for Ubiquitous Application"

[6] Wikipedia https://en.wikipedia.org/wiki/Digital_signature

[7] Parashar R, Parihar PS, Kurdia V. A Attack on E-Mail Encryption Protocols by Chosen Ciphertext Method. International Journal of Internet Computing. 2011; 1(1): 65-68.

[8] Prof. Patrick McDaniel, Network and Security Research Center Department of Computer Science and Engineering Pennsylvania State University, University Park PA – "Public-Key Cryptography and Attacks on RSA", 2010

[9] Federal Information Processing Standards Publications. 197. Advanced Encryption Standard. Washington DC: FIPS PUBS; 2001.
[10] Li B, Im EG. Smartphone, Promising Battlefield for Hackers. Journal of Security Engineering. 2011;8(1): 89-110.

Purevjav Saranzaya:

2012: B.S at Mongolian University of Science and Technology - School of Information and Telecommunication Technology
2014-current: M.S at Dongseo University, Republic of Korea
Research Area: Cryptographic, Network and Information Security.

TaeYong Kim

1993: B.S at Electrical Engineering from Fisheries University
1997: M.S at Electrical Engineering from Okayama University, Japan
2001: Ph.D at Electrical Engineering from Okayama University, Japan
2002-current: Professor of Dongseo University, Republic of Korea.

HoonJae Lee

1985: B.S at Kyungpook National University, Republic of Korea
1987:MS at Kyungpook National University, Republic of Korea
1998:Ph.D at Kyungpook National University, Republic of Korea
2002-current:Professor of Dongseo University, Republic of Korea
Research Interests: Password Theory, Network Security, Side-Channel Attack, Information Communication/ Information network.