ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Optimum Security Technique for Smart Phones

Renu Rani[1],Dr.Renu Bagoria[2]

P.G. Student, Department of Computer Engineering, Jagannath University, Chaksu, India[1]

Assistant Professor, Department of Computer Engineering, Jagannath University, Chaksu, India[2]

ABSTRACT: Securing mobile and smartphone data is vital issue in the communication industry and schemes that could be used to secure mobiles are not easy to implement and efficient so far. Securing data includes the messaging and additional application services on mobile devices. The applications available in market are not very reliable and surfing from issues of memory and resources. Additionally the security measures provided by smart phones are not enough to maintain the privacy of the data stored on the phone or protect it from falling in the wrong hands in case of mobile theft. Currently the security on smartphones is generally based on passwords and only effort made to secure the passwords is removing the dependency of characters and numbers. Due to the lack of security in small devices the need of proper security of data is required. The method that is able to secure data in efficient way and very hard to cheat other than the passwords, can be found by applying cryptography encryption algorithms. These encryption algorithms are very easy solutions to secure the data and as well not easy to break the security. There are two types of encryptions i.e. symmetric and asymmetric, in which the asymmetric cryptography encryption is better as it do not play with the security of data by using only one sided key because one sided keys are generally used in less secure areas. There are products available in market based on encryption but even those products are based on symmetric cryptography encryptions and we found that asymmetric cryptography algorithms are more secure to deploy on smartphones additionally we found that among them only one algorithm is powerful enough to deploy on these devices. These findings are based upon the comparison of algorithms in terms of memory and resources because most asymmetric encryption algorithms need large memory and heavy processor to use resources. We finally found that Elliptic curve cryptography algorithm is best among them to deploy on mobile devices as they have limited memory and resources.

KEYWORDS: encryption, decryption, cryptography, symmetric key, secrete key

I. INTRODUCTION

Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into anunreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text. Cryptography is a technique of hiding the plain information from the web. By using cryptography we can assist this shaky information by secrete writing on our computer network. Cryptography renders he message unintelligible to outsider by various transformations. Data Cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep the data secure from unauthorized access. In traditional (symmetric-key) cryptography, the sender and receiver of a message know and use the same secret key. The main challenge is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, a phone system, or some other transmission medium to prevent the disclosure of the secret key. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key. Because all keys in a secret-key (symmetric-key) cryptosystem must remain secret, secret-key cryptography often has difficulty providing secure key management. To solve the key management problem, Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography in 1976. Public-key cryptography refers to a cryptographicsystem requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. The algorithms used for public key cryptography are based mathematical relationships (the ones being the integer factorization and discrete logarithm problems).Although it is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

easy for the recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult for anyone to derive the private key, based only on their knowledge of the public key. This is why, unlike symmetric key algorithms, a public key algorithm does *not* require a secure initial exchange of one (or more) secret keys between the sender and receiver.In practice, only a hash of the message is typically encrypted for signature verification purposes.Public-key cryptography is a fundamental, important, and widely used technology. It is an approach used by many cryptographic algorithms and cryptosystems. Examples of well-regarded asymmetric key techniques for varied purposes include: Diffie–Hellman key exchange protocol, El Gamal, DSS (Digital Signature Standard), which incorporates the Digital Signature Algorithm, Various elliptic curve techniques, Various password-authenticated key agreement techniques, RSA encryption algorithm, Cramer–Shoup cryptosystem, YAK authenticated key agreement protocol. Among all RSA is most popular one. The proposed algorithm is similar with RSA with some modification. Proposed algorithm is also a public key cryptography algorithm. In this algorithm we have extremely large number that has two prime factors (similar to RSA).In addition of this we have used two public pair of keys. This modification increases the security of the cryptosystem.

II. CRYPTOGRAPHY AND TYPES

Cryptography uses the process of transposition and substitution of the characters to hide and retrieve the data. At the sender side we call it Encryption shown in Figure.1 and at the receiver side we called it decryption shown in Figure.2.We use the various keys to encrypt a decrypt the data. Keys are the special digital functions or methods that convert the plain text into inscribe format and its vice versa. Every element of the network have two keys namely private or personal key which is known to a particular person and public key which is known by all persons in the network. There are two types of cryptography.

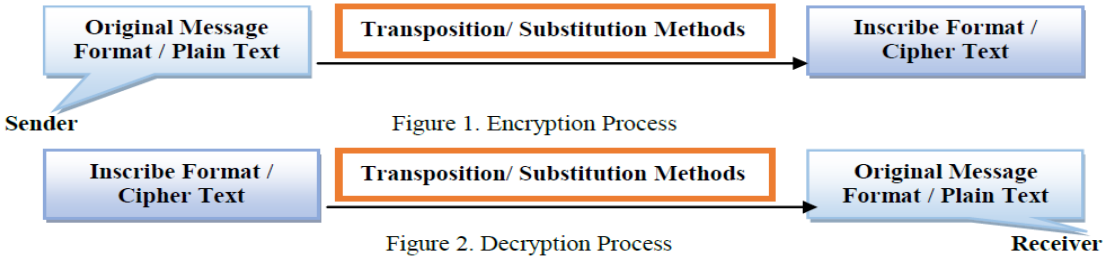

Figure 1. Encryption Process

Figure 2. Decryption Process

A. Same key cryptography or Private Key cryptography: In this type of cryptography the receiver and sender applies the same key to encrypt and decrypt the message or recover the plaintext from cipher text and vice versa, so this type of cryptography is also known as symmetric encryption and decryption.
the whole process of encryption and decryption can be carried out through receiver's private key. Through this cryptography form, it is obvious that the secret key must be known to both the sender and the receiver that why it is known as private key cryptography. Transmitting the secret key on insecure network can also destroy the security.

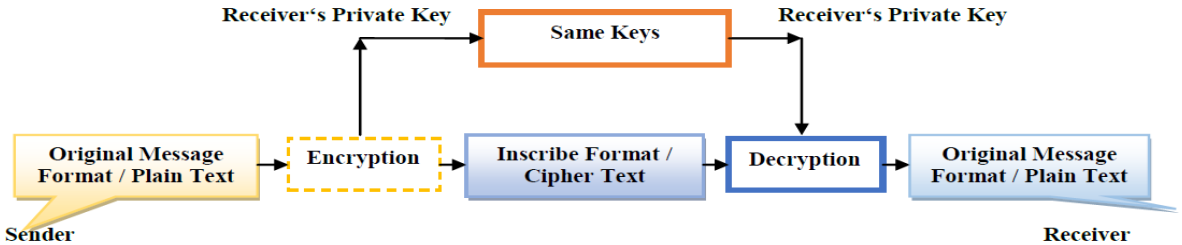

Figure3.Same key cryptography

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

*B. Different key cryptography or public key cryptography:*In this type of cryptography, the receiver and sender apply the Different keys to encrypt and decrypt the message or recover the plaintext from cipher text and its vice versa. This type of cryptography is also known as asymmetric encryption and decryption.Figure.4 is showing the whole process where receiver's public key is used for encryption and receiver's private key is used for decryption. In public key cryptography, each user or the workstation take part in the communication have a pair of keys, a public key and a private key and a set of operations associated with the keys to do the cryptographic operations. Only a particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Since the knowledge of public key does not compromise the security of the algorithms, it can be easily exchanged online.

III. ENCRYPTION IN RSA

The RSA algorithm [1] is a public key encryption algorithm which relies on the generation of two large prime numbers, and on the fact that their product is difficult to factorize. The standard RSA algorithm is divided into the following steps:

Step 1: Assume two large prime numbers **p** &**q**.

Step 2: Compute **N = p*q**, where **N** is a factor of two large prime numbers.

Step 3: Select an Encryption key **E** such that it is not a factor of the product **(p-1)*(q-1)** i.e., Ø(n)= (p-1)*(q-1); for calculating encryption exponents, **E** should be 1< E < Ø(n) such that gcd(E, Ø(n))=1.

Step 4: Select the Decryption key **D**, which satisfy the Equation D*E = 1 mod Ø(n).

Step 5: For Encryption: C=ME mod N, where C is Cipher text, M is Message.

a) Decryption

M= CD mod N.

b) *Security:*The Security of RSA mainly lies with the Selection of a large prime number, an Encryption Key and Decryption Key. Factoring large numbers is not provably hard, but no algorithms exists today to factor a 200-digit number in a reasonable amount of time.

The main feature of RSA algorithm is the selection of large prime number (p, q) because it is logical that fraction of large number is always typical and any users or force attackers could not be able to find the capable numbers, timely to force attack is shortly non-feasible.

c) *Advantages:*RSA's biggest advantage is that it uses Public Key encryption. This means that your text will be encrypted with someone's Public Key (which everyone knows about). However, only the person it is intended for can read it, by using their private key (which only they know about). Attempting to use the Public Key to decrypt the message would not work. RSA can also be used to "sign" a message, meaning that the recipient can verify that it was sent by the person they think it was sent by.

d) *Disadvantages:*A disadvantage of using public-key cryptography for encryption is speed. There are many secret-key encryption methods that are significantly faster than any currently available public-key encryption method. Nevertheless, public-key cryptography can be used with secret-key cryptography to get the best of both worlds. For encryption the best solution is to combine public and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. Public-key cryptography may be vulnerable to impersonation, even if users' private keys are not available.

IV. ENCRYPTION IN ECC

a) *Encryption:*Here, we essentially encode a message on the curve. Note that we cannot simply encode the message as the x or y coordinate of a point, because not all such coordinates are in **Ep(a, b)**, where **Ep(a, b)** denotes the elliptic group *mod* p whose elements (x, y) are pairs of nonnegative integers less than p, satisfying:

y2 = x3 + ax + b (mod p)

As with the Key Exchange system, an Encryption/Decryption [4], [6], [8] system requires a point P and an elliptic group as parameters. Each user A selects a private key **d** and generates a public key as follows

Q = d * P where **d** = The random number that we have selected within the range of **1 to (n-1)**.

P is the point on the curve.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Q is the public key and '**d**' is the private key.
Consider 'm' has the point 'M' on the curve 'E'. To encrypt and send a message M to B, A chooses a random positive integer 'k' from 1 to (n-1) and produces the Ciphertext as a pair of points. Let the two points be Ca and Cb. The Ciphertext can be represented as
Cm = { Ca, Cb }
whereCa = k*P
Cb = M + k*Q
Cm will be sent.
Important thing to note is that A has used B's public key Q.

b) *Decryption:*To recover the message M, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:
M = Cb – d * Ca

c) *Security:* A has masked the message M by adding k*Q to it. Nobody but A knows the value of 'k', so even though Q is a public key, nobody can remove the mask k*Q. However, A also includes a "clue," which is enough to remove the mask if one knows the private key 'd'. For an attacker to recover the message, the attacker would have to compute 'k' given P and k*P ,which is hard.

d) *Advantages:* ECC employs a relatively short encryption key, a value that must be fed into the encryption algorithm to decode an encrypted message. This short key is faster and requires less computing power than other first-generation encryption public key algorithms. For example, a 160-bit ECC encryption key provides the same security as a 1024-bit RSAencryption key and can be up to 15 times faster, depending on the platform on which it is implemented. The advantages of ECC over RSA are particularly important in wireless devices, where computing power, memory and battery life are limited.

e) *Disadvantages:* One of the main disadvantages of ECC is that it is more complex and more difficult to implement than RSA, which increases the likelihood of implementation errors, thereby reducing the security of the algorithm.

V. RESULTS & DISCUSSIONS

We have tested the implementation of RSA and ECC cryptosystems separately. The tests are done for the following parametric factors and the results are shown

Message	RSA(cipher text)	Ecc(cipher text)
12345678909876543210123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210	21869679730177211594340937376330861577389571072633039576701618112034364399557542245964834233662262961427730852537713233595146674268216072108918510727434321621598117646881464362265274656863225532991639153199739154729548054973536585359308851128092407277096145875949955352570397278995776154366318691615132488473	304402205a1feae16f5d65437405203a9dea9fcd55afaf4fc2c38c094259819a33871c9c02206d7395db41bd4aaa90cb9d859bf5407c3da4bedb7cb886f21ba39d8f0e2cb2d4

Time taken by both RSA and ECC for creating the above cipher text:

RSA(time taken in miliseconds)	ECC(time taken in miliseconds)
1170	62

Our findings suggest that RSA key generation is significantly slower than ECC key generation for RSA key of sizes 1024 bits and greater. Considering there are affordable devices that can break RSA keys smaller than 1024 bits in a

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

matter of days, the cost of key generation can be considered as a factor in the choice of public key systems to use when using digital signatures, especially for smaller devices with lesser computational resources.
The difference in their key sizes grows exponentially to maintain the same relative power as compared to the average computing power available. In fact, RSA Security on their own have admitted on their website that ECC is the technique to be in demand in the future. However, the fact remains that ECC was discovered during the process of trying to find out new ways to attack on systems using RSA techniques. This time difference in RSA and ECC clearly suggests that ecc is way far faster than the rsa algorithm and hence can be easily deployed on smart phones and with the same level of security.

VI. CONCLUSIONS

We have studied all aspects of security of mobile devices in various fields of mobile services i.e. SMS, MMS and applications and we have now reached to a level to decide that all the services are dependent on the layered architecture that works on a platform which is the most efficient way to understand the deployment of the working of securing techniques. This leads us to find out the finest methods of security in mobile devices i.e. smart phones which are capable to run securing techniques with sufficient hardware needs according to the need of techniques for testing and running application which was only possible by following an efficient algorithm technique that can be deploy on mobile platform because Smartphone have very sufficient memory and small CPU clock cycle to handle the processing. We compared best encryption algorithms according to our need with understanding their the base concepts. There exist both symmetric and asymmetric algorithms that can be implemented efficiently on a mobile phone for the purposes of securing the content during both transmission and in storage within the limited resources; we conclude that it is feasible. The feasibility of these findings however only extends as far as the sample content that were sourced. It is recommended that the system is tested on a wider range of contents in order to determine its feasibility on a broader scope. We then finally compared RSA and ECC algorithm best in their work for finding the best algorithm and understanding the need of our chosen one. Later we concluded that with very small processor and CPU clock cycle and memory need ECC algorithm fits itself in accordance to our need of the security. So our final conclusion is that we can deploy the ECC algorithm in accordance to our need of securing the services of mobile i.e. SMS, MMS and applications as best algorithm that works very efficiently with small hardware and very difficult to crack the security.

REFERENCES

[1] Gururaja, H.S., Seetha, M., Koundinya, A.K., "Design and Performance Analysis of Secure Elliptic CurveCryptosystem", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, 2013.
[2] PriitKaru, JonneLoikkanen, "Practical Comparision of Fast Public-Key Cryptosystems", Tik-110.501 Seminar on Network Secrity, 2000.
[3] Sonal Sharma, Jitendra Singh Yadav and Prashant Sharma, "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012.
[4] Gagandeepshahi, Charanjitsingh "Cryptography and its two Implementation Approaches" International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 1, Issue 3, May 2013
[5]http://www.scribd.com/doc/55154238/31/DISADVANTAGES-OF-RSA
[6] Implementation of elliptic curve cryptography on text and image International Journal of Enterprise Computing andBusiness Systems, ISSN (Online): 2230-8849, Vol. 1 Issue 2, 2011
[7]Wikipedia.orghttp://en.wikipedia.org/wiki/Cryptography
[8] Peersman C., Cvetkovic S., Griffiths P. and Spear H., "The global system for mobile communications short message service", IEEE Trans. Personal Commun., Vol. 7, pp. 15-23, June 2000.