Compartition of different Cryptographic Algorithms for Security of Mobile Portable Devices

Miss Rashmi Shinde, Prof. Sanjay Pawar***

**Department of E&TC, BVCOE, Kolhapur, M.S. India*
***Department of E&TC, BVCOE, Kolhapur, M.S. India*

Abstract

Use of mobile and portable devices are increasing in day today's life for business, domestic, banking, military, ministry purpose. As these are portable devices one use to store personal and sensitive information on the device. Hence these devices require strong security from intruders. In this paper we discuss about hardware and software securities provided for the devices through HSM, TPM and different cryptographic algorithms. In short we are starting from the basic of cryptography move towards comparision of different cryptographic algorithm and conclude the best suitable approach for the security purpose. In the IT world, strong security demands are satisfied by cryptographic solutions.

Keywords

Security, Encryption, Decryption, TPM, Symmetric key, Elliptical curve cryptography.

1.Introduction

. Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography is writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

1.Authentication*:* The process of proving one's identity.

2. Privacy/confidentiality*:* Ensuring that no one can read the message except the intended receiver.

3.Integrity: Assuring the receiver that the received message has not been altered in any way from the original.

4.Non-repudiation*:* A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into *ciphertext*, which will in turn (usually) be decrypted into usable plaintext.

In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common nomenclature in the crypto field and literature to make it easier to identify the communicating parties. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party.

2. What is mean by Encryption Decryption?

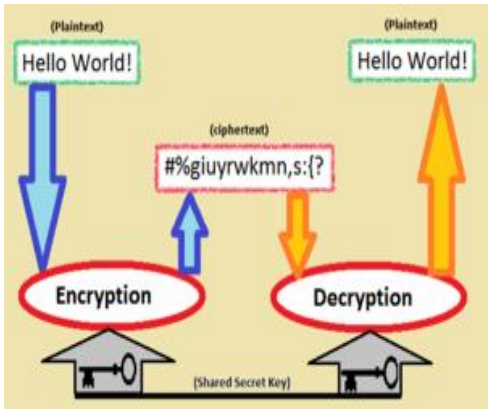

Fig1:Encryption Decryption process

Encryption is the conversion of data into a form, called a cipher, that cannot be understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. Encryption and decryption should not be confused with encoding and decoding, in which data is converted from one form to another but is not deliberately altered so as to conceal its content.[8]

A data encryption/decryption IC is a specialized integrated circuit (IC) that can encrypt outgoing data and decrypt incoming data. Some such devices are intended for duplex operation (in which input and output do not occur simultaneously), and others are designed for full-duplex operation (where input and output can occur simultaneously).

The increasing need for strong security applications that are fast and compromise resistant has led to the development, over time, of a wide range of hardware cryptographic processor devices. A typical cryptographic processor is a physically tamper-resistant embedded processor which communicates to a conventional general purpose processor system and offers a predefined set of cryptographic services. The first commercial uses of cryptographic processors or Hardware Security Modules (HSM), were made for financial transactions. Traditionally, in such applications, HSMs enforced a policy on key usage along with a series of key protection measures. Electronic payment systems use the HSM for secure communication between the banks and the merchants and to securely store all needed authentication information. This financial system also includes the customer side by providing to the customer a cheap autonomous HSM (smart card) along with a Personal Identification Number (PIN). This smart card solution guarantees end-to-end security in the communication between the bank and its clients. After the introduction of Internet banking in the financial world, the above security solution was not enough since the user no longer needed to be physically present in a prearranged place to use the bank services. The ubiquitous nature of banking through the internet, created the need for an island of trust regardless of the user's location or the means by which a potential transaction is made. This challenge is currently met by issuing tamper resistant authentication – authorization devices (e.g. the RSA Secured) that can provide time-dependent or random passwords based on unique registered key in the device. The emerging trend of embedded system designs for a wide variety of commercial products (smart grid, automotive applications e.t.c.) has also created a need for strong security . In such systems security is managed and maintained by hardware means. HSM for embedded systems need to incorporate a great number of security characteristics in order to instill trust to the user and stakeholder community. Public Key Interface, Digital signature verification, key agreement distribution, secure storage, tamper evidence, detection and resistance are key services that the upcoming new generation of HSMs will offer. [1]

3.Hardware structures

- USB tokens
- Smart cards
- Specialized security chips
- PIN

Fig 2:smart cards ,HSM

A **hardware security module** (**HSM**) is a type of secure cryptoprocessor targeted at managing digital

keys, accelerating cryptoprocesses in terms of digital signings/second and for providing strong authentication to access critical keys for server applications. These modules are physical devices that traditionally come in the form of a plug-in card or an external TCP/IP security device that can be attached directly to the server or general purpose computer. Modules are also deployed in the form of network HSMs to manage Transparent Data Encryption keys associated with some databases.[8]

The goals of an HSM are (a) onboard secure generation, (b) onboard secure storage, (c) use of cryptographic and sensitive data material, (d) offloading application servers for complete asymmetric and symmetric cryptography. HSMs provide both logical and physical protection of these materials from non-authorized use and potential adversaries. In short, they protect high-In computing,

4.Trusted Computing Solution and Trusted Platform Module:

The evolution of malicious attacks and behaviors in computing system has disturbed the trust that users have to their computing devices. The user no longer believes that the information provided by his device or another user's device is not tampered with or compromised. In order to match the demanding need for more sophisticated HSMs capable of providing a trust island in an existing untrusted environment, the Trusted Computing Group (TCG) industry consortium, was founded. This consortium is responsible for formalizing, applying, and extending the trusted computing ideas to wellknown and established computer systems either by introducing new hardware or software modules or by proposing appropriate protocols for those modules. Trusted Computing can be viewed as a collection of technologies capable of constantly monitor the behavior of a given computer system for indication of a possible compromise. The core of this technology is embodied in a HSM, denoted as Trusted Platform Module (TPM) . [2]

4.1TPM:Trusted Platform Module

Trusted Platform Module (TPM) is both the name of a published specification detailing a secure crypto processor that can store cryptographic keys that protect information, and the general name of implementations of that specification, often called the "TPM chip" or "TPM Security Device". The TPM specification is the work of the Group value cryptographic keys.

The TPM is a smart-card like hardware chip that is bound to the computer system (usually soldered on the system's motherboard). In its current version (TPM 1.2), the chip is equipped with all the necessary components in order to support strong security features. Apart from the I/O interface, necessary for the TPM communication with the external world, inside the TPM there are a series of cryptographic hardware components including a true random generator unit, a digital signature and authentication-authorization scheme unit based on public key cryptography and hash function. At the moment, the TPM functionality supports only the RSA algorithm with 2048 bit keys and 160 bit hashing through SHA 1 algorithm. The TPM also supports the secure storage of security-sensitive values (like public - private key pairs or measurement states) in special memory units. Those memory units are a non-volatile, secure memory and a series of special purpose Platform Configuration Registers (PCR) that can only store an extended version of their previous values (usually a hashing of their previous value). All those units are tamper resistant and are protected from invasive and non invasive hardware attacks.[2]

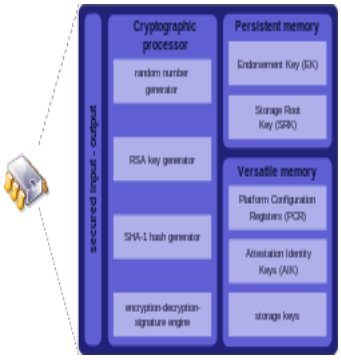

Fig3.internal of TPM

5.Software solutions

- Digital signature
- Cryptographic algorithms

5.1DSS:Digital signature standards

NIST: National institute of standards & technology published the DSS standards in 1991 & revised in 1993 & 1996. NIST is recommending the use of 2,048 bit RSA keys from year 2010 performance at longer key sizes is becoming increasingly important. DSS electronically signs the electronic messages, documents, transactions.

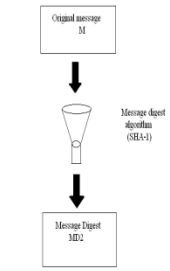

Fig-Receiver calculates its own Message digest

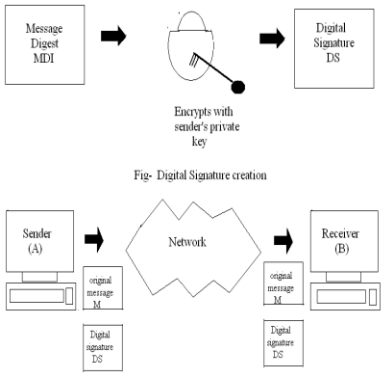

Fig- Digital Signature creation

Fig4.DSS

Disadvantages of DSS

1.They are slow.
2. Not secure
3.Less flexible as compared to key algorithms

5.2 Symmetric key algorithm

A secret key algorithm is symmetric, (or) it uses same key for encryption and also for decryption. The security of secret key algorithm rests with keeping key itself. Completely secret from others. Public key algorithm use different keys for encryption an decryption one key caused private key, must kept secret by its owner and in general is never shared with anyone else. The other key called public key will be shared with anyone else. The two will be mathematically related.

If we want to send message quickly we use Symmetric key algorithm.

5.3Asymmetric key algorithm

One key for Encryption & one key for Decryption. If we want to send messages secretly we use public key. In a classic cryptosystem, we have encryption functions E_K and decryption functions D_K such that D_K(E_K(P)) = P for any plaintext P. In a public-key cryptosystem, E_K can be easily computed from some "public key" X which in turn is computed from K. X is published, so that anyone can encrypt messages. If decryption D_K cannot be easily computed from public key X without knowledge of private key K, but readily with knowledge of K, then only the person who generated K can decrypt messages. That's the essence of public-key cryptography, introduced by Diffie and Hellman in1976.

Key exchange, of course, is a key application of public-key cryptography (no pun intended). Asymmetric schemes can also be used for non-repudiation; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message. Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography

Disadvantages of key algorithm

1.Key distribution problem is major disadvantage.
2.Key length is too large
3Less flexible
4.There is a problem of secret writing

6.Consideration of more improved Cryptographic Algorithm

The purpose of cryptography is to transmit information in such a way that access to it is restricted entirely to the intended recipient. Originally the security of a crypto text depended on the secrecy of the entire encrypting and decrypting procedures; however, today we use ciphers for which the algorithm for encrypting and decrypting could be revealed to anybody without compromising the security of a particular cryptogram. In such ciphers a set of specific parameters, called a **key**, is supplied together with the plaintext as an input to the encrypting algorithm, and together with the cryptogram as an input to the decrypting algorithm. The encrypting and decrypting algorithms are publicly announced; the security of the cryptogram depends entirely on the secrecy of the key, and this key must consist of any **randomly** chosen, sufficiently long string of bits. Once the key is established, subsequent communication involves sending cryptograms over a public channel which is vulnerable to total passive eavesdropping (e.g. public announcement in mass-media). However in order to establish the key, two users, who share no secret information initially, must at a certain stage of communication use a reliable and a very secure channel. Since the interception is a set of measurements performed by the eavesdropper on this channel, however difficult this might be from a technological point of view, **in principle** any **classical** key distribution can always be passively monitored, without the legitimate users being aware that any eavesdropping has taken place.

Mathematicians have tried hard to solve the key distribution problem. The 1970s brought a clever mathematical discovery in the shape of ``public key'' systems. In these systems users do not need to agree on a secret key before they send the message. They work on the principle of a safe with two keys, one public key to lock it, and another private one to open it. Everyone has a key to lock the safe but only one person has a key that will open it again, so anyone can put a message in the safe but only one person can take it out. These systems exploit the fact that certain mathematical operations are easier to do in one direction than the other. The systems avoid the key distribution problem but unfortunately their security depends on unproven mathematical assumptions, such as the difficulty of factoring large integers (RSA - the most popular public key cryptosystem gets its security from the difficulty of factoring large numbers. This means that if and when mathematicians or computer scientists come up with fast and clever procedures for factoring large integers the whole privacy and discretion of public-key cryptosystems could vanish overnight. Indeed, recent work in quantum computation shows that quantum computers can factorize much faster than classical computers.

6.1Trusted Computing on Mobile – Portable platforms.

While the TCG initiative has established a good market base in desktop and laptop computers, there is no imminent adoption-commercialization of this technology by the mobile, portable industry due to several TPM restrictions in terms of usability, flexibility and user freedom. This trend is mirrored in the small adoption of the mobile version of the TPM, denoted as MTM (Mobile Trusted Module). This module, specified to provide all TCG functionality along with additional encryption/decryption services, has to operate under a very constrained chip covered area and power dissipation environment without compromising its computational speed.
As a result of the above, fitting a trusted computing hardware architecture, like the TPM-MTM hardware structure, in a mobile, portable device can be a very challenging design and implementation action bearing a considerable cost on the manufacturer side, a cost that is bound to slide to the customers.[4,5,6]

Apart from the implementation constrains due to the mobile, portable hardware environment, the existing approach on trust enforcement for mobile-portable systems through hardware means, based on TCG's existing specifications, suffers from another serious problem. The tightly bound cryptographic framework (restricted on AES, RSA and SHA- 1 algorithms) under which the security mechanisms are applied can be very limiting on the possible supplied services and cannot be upgraded to better security schemes. Thus, current trusted computing hardware structures are lacking algorithm and security flexibility so as to support a wide range of possible trust levels and security services. When the existing algorithms are outdated then the mobile systems using them will be rendered useless or at least insecure untrusted.[1]

Thus the above stated cryptographic algorithms along with hardware structures have some limitations while implementing in mobile as we have to considor size

and power required for environment. The design of a strong security-trust assurance HSM for portable systems can be made possible by considoring the following points
Use of modern and mature Cryptographic Algorithms. Security flexibility by use of more versatile protocols.

To match these requirements the designers need to consider todays implemented ande existing MTM – TPM solutions and adopt more efficient cryptographic schemes. Researchers point to Elliptic Curve cryptography as the most suitable candidate for a public key scheme and to SHA256 or the upcoming SHA3 as the most suitable Hash function scheme . Elliptic Curve cryptography (ECC) is a mature public key cryptographic toolset that has been researched extensively in parallel to RSA. It provides hardware implementations that are smaller in chip covered area and power dissipation in comparison to RSA. The main reason for such feat is the fact that ECC can offer the same security level as traditional public key cryptographic schemes (like RSA) but with considerably smaller key sizes. In contrast to RSA, the ECC mathematic toolset is very broad and can support a big number of security protocols thus providing flexibility and versatility.[1]

7.Eliptical curve cryptography:

In 1985, Elliptic Curve Cryptography (ECC) was proposed independently by cryptographers Victor Miller (IBM) and Neal Koblitz (University of Washington). ECC is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP)

In general, public-key cryptography systems use hard-to-solve problems as the basis of the algorithm. The most predominant algorithm today for public-key cryptography is RSA, based on the prime factors of very large integers. While RSA can be successfully attacked, the mathematics of the algorithm have not been comprised, per se; instead, computational brute-force has broken the keys. The defense is "simple" — keep the size of the integer to be factored ahead of the computational curve! In 1985, Elliptic Curve Cryptography (ECC) was proposed independently by cryptographers Victor Miller (IBM) and Neal Koblitz (University of Washington). ECC is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Like the prime factorization problem, ECDLP is another "hard" problem that is deceptively simple to state: Given two points, P and Q, on an elliptic curve, find the integer *n*, if it exists, such that p= nQ. Elliptic curves combine number theory and algebraic geometry. These curves can be defined over any field of numbers (i.e., real, integer, complex) although we generally see them used over finite fields for applications in cryptography. An elliptic curve consists of the set of real numbers (x, y) that satisfies the equation:

$$y^2 = x^3 + ax + b$$

The set of all of the solutions to the equation forms the elliptic curve. Changing *a* and *b* changes the shape of the curve, and small changes in these parameters can result in major changes in the set of (x,y) solutions.

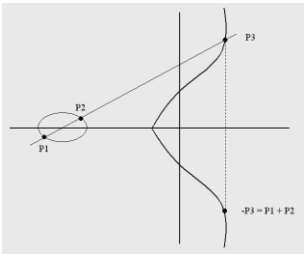

Fig5.addition of two points usin ECC

zP, *or*, Q = nP. An attacker might know P and Q but finding the integer, *n*, is a difficult problem to solve. Q is the public key, then, and *n* is the private key.[7]

Advantages of Elliptical curve cryptography

1. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.
2. Mature public key cryptography.
3. Small area requirement for hardware coverage.
4. Less power dissipation.
5. Flexibility & versatility.

7.1 COMPARISION OF DIFFERENT ALGORITHMS ACORDING TO CRYPTOGRAPHIC STRENGTH

SYMMETRIC KEY ALGORTHM	56	80	112	128	192	256
RSA	512	1024	2048	3072	7680	15360
ECC	112	161	224	256	384	512
KEY RATIO	5:1	6:1	9:1	12:1	20:1	30:1

CONCLUSION:

In this paper, we discuss what is mean by encryption decryption. The hardware modules provided for the security purpose using TCG's. After we compare different security algorithms and discussed how elliptical curve cryptography is the best suitable option as far as software solutions are considered.

.

References:

1. A.P. Fournaris "Towards flexible security and trust hardware structures for mobile portable systems" IEEE Latic Amerika Transactions, Vol 10, No3, april 2012.

2. TCG Trusted Computing Group TPM Main part 2 TPM Structure specification version 1.2

3. A.P. Fournaris and D. M. Hein "Reust management through Hardware means design concerns and optimization in VLSI 2010 annual symposiam Vol 105 N Voros, A Mukharjee N Sklavos K Masselos and Mhuebner, Eds springer, Netherlands 2011"

4 J.Grosschadl ,T.Vejda and D.Page,"Reassessing the TCG specifications for trusted computing in mobile and Embeded systems"in2008

5. A. U. Schimidt, N. Kuntze and M. Kasper, "On the deployment of Mobile Trusted Modules " Fraunhofer Institute for Secure, pp. 134-140, Feb 2010

6. M Kim, H ju, Y Kim, J Park and Y Park, "Design and Implementation of Mobile Trusted Modules for Trusted Mobile Computing". IEEE Transactions on consumer Electronics Vol 56 Feb 2010

7. Atul Kahate, "Cryptography and Network Security"

8. Hardware Security Module

"http://en.wikipedia.org/w/index.php?title=Hardware_security_module&oldid=493861420"