ISSN:0975-9646

The Prototype for the Unification of Various Cryptographic Modules: A Solution to the Information Security

Sani Asnain wani, Iqbal Ali, Dr. Abdul Raouf Khan

Department of Computer Science,
King Faisal University

Abstract:-In this paper, we have proposed the concept for the unification of various cryptographic modules. By applying this concept, the software engineers can develop an application which can perform both the encryption and decryption of various types of files. We have chosen java as the base of our study. It is because the java platform strongly emphasizes security, including language safety, cryptography, authentication, public key infrastructure and access control. Apart from discussing this concept, we have defined some technical terms more precisely for understanding the concept properly.

Keywords: Cryptography and Modern Cryptography, Confidentiality, Data Integrity, Authentication, Nonrepudiation, JCA and JCE.

CRYPTOGRAPHY AND MODERN CRYPTOGRAPHY:

The Concise Oxford Dictionary (2006) defines cryptography as the art of writing or solving codes. This definition may be historically accurate, but it does not capture the essence of modern cryptography. First, it focuses solely on the problem of secret communication. This is evidenced by the fact that the definition specifies "codes", elsewhere defined as "a system of pre-arranged signals, especially used to ensure secrecy in transmitting messages". Second,the definition refers to cryptography as an art form. Indeed, until the 20thcentury (and arguably until late in that century), cryptography was an art.Constructing good codes, or breaking existing ones, relied on creativity and personal skill. There was very little theory that could be relied upon and there was not even a well-defined notion of what constitutes a good code.In the late 20th century, this picture of cryptography radically changed. A rich theory emerged, enabling the rigorous study of cryptography as a science. Furthermore, the field of cryptography now encompasses much more than secret communication. For example, it deals with the problems of message authentication, digital signatures, protocols for exchanging secret keys,authentication protocols, electronic auctions and elections, digital cash and more. In fact, modern cryptography can be said to be concerned with problems that may arise in any distributed computation that may come under internal or external attack. Without attempting to provide a perfect definition of modern cryptography, we would say that it is the scientific study of techniques for securing digital information, transactions, and distributed computations.

Another very important difference between classical cryptography (say, before the 1980s) and modern cryptography relates to who uses it. Historically,the major consumers of cryptography were military and intelligence organizations. Today, however, cryptography is everywhere! Security mechanisms that rely on cryptography are an integral part of almost any computer system. Users (often unknowingly) rely on cryptography every time they access a secured website. Cryptographic methods are used to enforce access control in multi-user operating systems, and to prevent thieves from extracting trade secrets from stolen laptops. Software protection methods employ encryption,authentication, and other tools to prevent copying. The list goes on and on.

In short, cryptography has gone from an art form that dealt with secret communication for the military to a science that helps to secure systems for ordinary people all across the globe. This also means that cryptography is becoming a more and more central topic within computer science [1].

In this paper our discussion revolves around the Modern Cryptography in order to achieve the following aspects:

- Confidentiality or privacy,
- Data integrity,
- Authentication,
- Nonrepudiation.

Each of these aspects of module security can be addressed by standard methods in cryptography.

ENCRYPTION:

The process of disguising a message so as to hide the information it contains;this process can include both encoding and enciphering [2].

Encoding means to convert a message into a representation in a standard alphabet, such as to the alphabet {A. . . Z} or to numerical alphabet.

Enciphering means to convert plaintext into ciphertext.

DECRYPTION:

All three terms - decipher, decrypt, and decode - mean to convert ciphertext into the original, unencrypted plaintext. Decrypt is actually a generic term, covering both the other terms, that simply means to unscramble a message. [3]

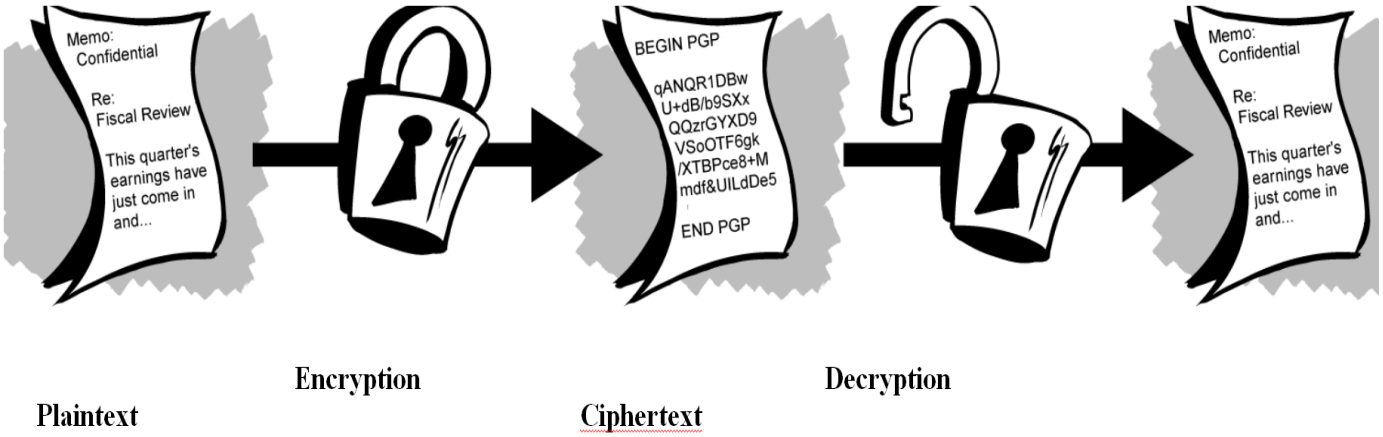

Figure 1. Encryption and decryption

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher -- that is, the harder it is for unauthorized people to break it -- the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including that of the United States, want to set up a key-escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could hack into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption.

Figure1 is the illustration of the encryption and decryption process.

It should be noted that there are various ways of encrypting and decrypting the data, but we don't want to discuss those various types of encryption and decryption in this paper.

STEGANOGRAPHY:

Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography's goal is to keep its mere presence undetectable, but steganographic systems— because of their invasive nature— leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called statistical steganalysis [4]. Figure 2 illustrates the process of the steganographic system.

Now we want to discuss all of the elements necessary for secure communication over an insecure channel, namely Confidentiality (Privacy), Data Integrity, Authentication and Non-repudiation.

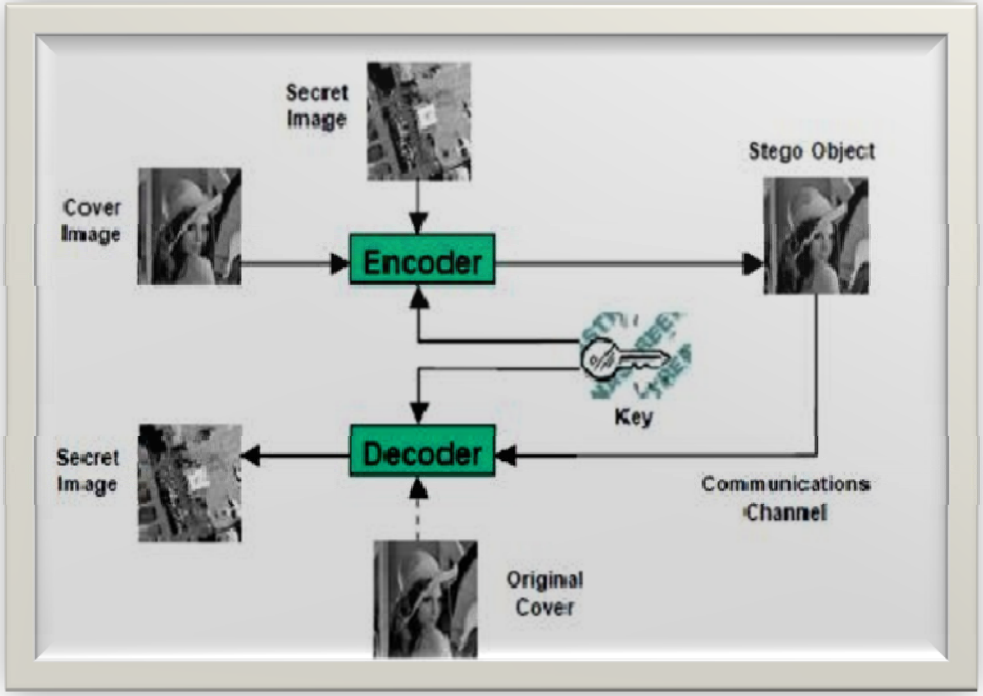

Figure 2. An example of steganography.

CONFIDENTIALITY:

Confidentiality refers to limiting information access and disclosure to authorized users -- "the right people" -- and preventing access by or disclosure to unauthorized ones -- "the wrong people."

Underpinning the goal of confidentiality are authentication methods like user-IDs and passwords, that uniquely identify a data system's users, and supporting control methods that limit each identified user's access to the data system's resources [5].

Also critical to confidentiality, data integrity, Authentication and Non-repudiation as well -- are protections against malicious software (malware), spyware, spam and phishing attacks.

Confidentiality is related to the broader concept of data privacy -- limiting access to individuals' personal information.

DATA INTEGRITY

Integrity refers to the trustworthiness of information resources.

It includes the concept of "data integrity" -- namely, that data have not been changed inappropriately, whether by accident or deliberately malign activity. It also includes "origin" or "source integrity" -- that is, that the data actually came from the person or entity you think it did, rather than an imposter.

Integrity can even include the notion that the person or entity in question entered the right information -- that is, that the information reflected the actual circumstances (in statistics, this is the concept of "validity") and that under the same circumstances would generate identical data (what statisticians call "reliability").

On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong [5].

AUTHENTICITY

Refers to the reliability of the data in a broad sense. Defining and assessing authenticity is a complex task,

which includes defining of roles, policies, components, and protocols for the custodial function. Authenticity is never limited to the resource itself, but is rather extended to the information /document/record system, and thus to the concept of reliability: authenticity is concerned with ongoing control over information/document/record creation process and custody. The verification of the authenticity of a resource is related to the reliability of the system/resource. Authenticity is established by assessing the integrity and identity of the resource. [6]

NON-REPUDIATION

Repudiation is the denial by one of the entities involved in a communication or part of the communication. Non-repudiation is concerned with preventing such a denial. With sender non-repudiation, the originator of a data exchange is provided with a *proof of receipt* (POR) which proves that the recipient received the data. Receiver non-repudiation provides the recipient with a *proof of origin* (POO) which proves that the originator sent the data. The proofs of origin

and receipt constitute non-repudiation evidence information. Principals can exchange evidence information, either through direct peer-to-peer communication or indirectly via a third-party intermediary (see figure 3).[7]

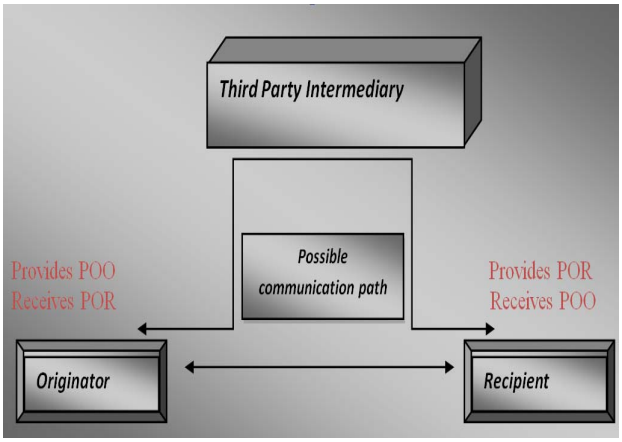

Figure 3. Non-Repudiation Service.

After discussing these fundamental elements required for secure communication we want to give a basic introduction about JCA and JCE.

JAVA CRYPTOGRAPHY ARCHITECTURE (JCA):

The JCA is a major piece of the java platform, and contains a "provider" architecture and a set of APIs for digital signatures, message digests (hashs), certificates and certificate validation, encryption (symmetric/asymmetric block/stream ciphers), key generation and management, and secure random number generation. These APIs allow developers to easily integrate security into their application code. The architecture was designed around the following principles:

1. **Implementation independence**
   Applications do not need to implement security algorithms. Rather, they can request security services from the Java platform. Security services are implemented in providers (see below), which are plugged into the Java platform via a standard interface. An application may rely on multiple independent providers for security functionality.
2. **Implementation interoperability**
   Providers are interoperable across applications. Specifically, an application is not bound to a specific provider, and a provider is not bound to a specific application.
3. **Algorithm extensibility**
   The Java platform includes a number of built-in providers that implement a basic set of security services that are widely used today. However, some applications may rely on emerging standards not yet implemented, or on proprietary services. The Java platform supports the installation of custom providers that implement such services.

Architecture

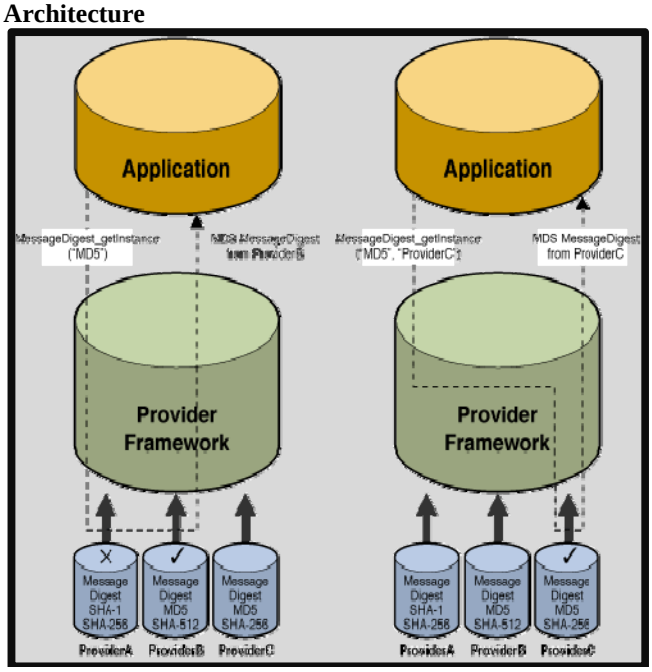

Figure 4. Java Cryptography Architecture

The JCA offers a set of APIs that allow users to query which providers are installed and what services they support.
This architecture also makes it easy for end-users to add additional providers. Many third party provider implementations are already available.[8]

JAVA CRYPTOGRAPHY EXTENSION:

The Java Cryptography Extension (JCE) extends the JCA API to include APIs for encryption, key exchange, and Message Authentication Code (MAC). Together, the JCE and the cryptography aspects of the SDK provide a complete, platform-independent cryptography API. JCE was previously an optional package (extension) to the Java 2 SDK, Standard Edition, versions 1.2.x and 1.3.x. JCE has now been integrated into the Java 2 SDK, v 1.4.

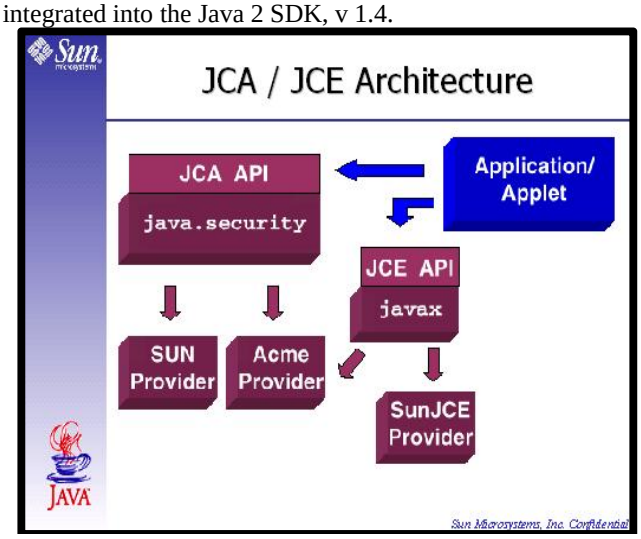

Figure 5. Java Cryptography Extension

GRAPHICAL REPRESENTATION:

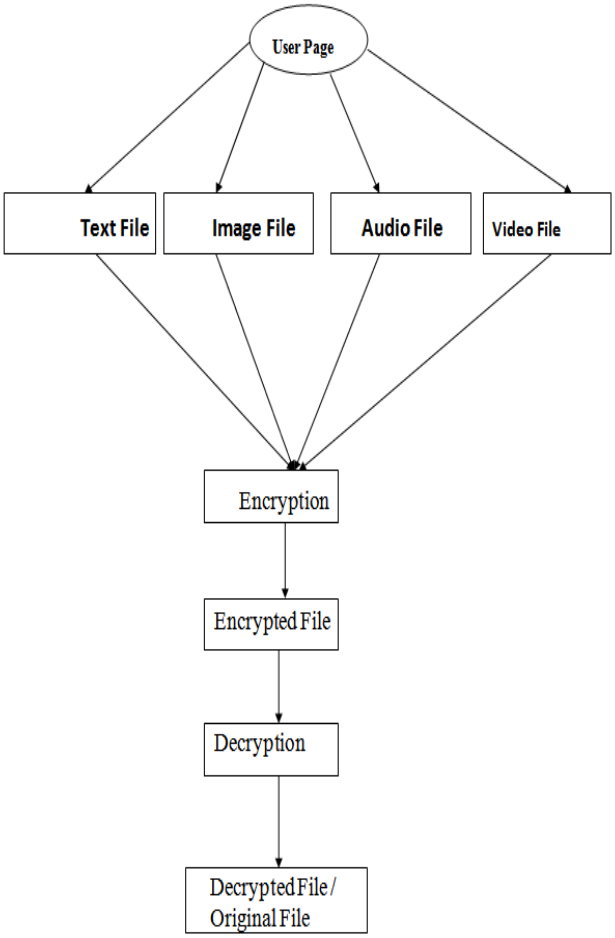

Figure 6. Data Flow Diagram

MODULE DESCRIPTION:

User Page: This module is required to login the authorized user and sign up for the new user.

Files:
This module is for selecting the specific type of file, as you can see in the DFD that we can save the information in different formats, so we need a module using which we can select the required file for encryption.

Encryption: In this module we can implement different types of algorithms for encrypting the different types of files.

Decryption: This module is required for decrypting the encrypted files in order to bring them in the readable format or we can say in their original form.

Classes used for encryption and decryption:

Given below is the list of inbuild classes in java that can be used for the process of encryption and decryption of various types of files.

- **FileInputStream**
- **File**
- **FileOutputStream**
- **Cipher**
- **KeyGenerator**
- **SecretKey**
- **CipherInputStream**
- **CipherOutputStream**

CONCLUSION:

As we know that in the present world, the efficiency of the software is not sufficient for evaluating its quality .The quality of the software demands both the efficiency and the security. Keeping this thing in view we have discussed in our paper about the integration of various cryptographic modules in order to produce an efficient and adequately secured unified module. It should be noted here that by integration we do not simply mean to join the different working modules, but it also includes the robustness and the reliability of the integrated modules.

REFERENCES

1. *Introduction to Modern Cryptography www.cs.biu.ac.il/~lindell/Intro**ModernCryptography-Chapter1.pdf***
2. Math3024 Elementary Cryptography and Protocols *echidna.maths.usyd.edu.au/kohel/tch/MATH3024/.../lectures_01.pdf*
3. *http://searchsecurity.techtarget.com/definition/decryption*
4. *Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography" ,* IEEE SECURITY & PRIVACY, 1540-7993/03 © 2003 IEEE.
5. University Of Miami, "Privacy/ Data Protection Project". *http://privacy.med.miami.edu/glossary/xd_confidentiality_integrity_availability.htm*
6. Authenticity and Provenance in Long Term Digital Preservation: Modeling and Implementation in Preservation Aware Storage http://static.usenix.org/event/tapp09/tech/full_papers/factor/factor.pdf
7. NON-REPUDIATION WITH MANDATORY PROOF OF RECEIPT *http://www.cs.uccs.edu/~cchow/pub/security/nonRepudiation/ACMSigCommReview96p6-coffey.pdf*
8. *http://docs.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html*