Abstract— In today’s world communication mobile computing device has increased a lot. However, the communication over the mobile device must be secure. There must be secure transfer of information in order to provide Security, integrity and secure message transfer. HTTPS might not be sufficient. Developer needs to take the help of various cryptographic packages. These packages are available as Third party mobile cryptographic toolkit. This paper shows a comparison of various algorithms that are included in the bouncy castle toolkit. There key generation and relative study of both Symmetric and Asymmetric algorithm perform and will proves which algorithm is better and efficient.

Keywords— Bouncy castle toolkit, Encryption algorithm, Mobile Cryptography package;

I. INTRODUCTION

Java 2 Micro Edition or J2ME is type of Operating Platform work with Java Programming. This J2ME is incorporated with mobile device include smart phone. This J2ME contain Multiplicity of Application. The J2ME is java Specification for device with Low Memory and other constraint. It means it is used for cell phone programming.

The java 2 platform has several editions, including Enterprise Edition (J2EE) for the Server side and Standard Edition for the (J2SE) for the Desktop System. J2ME is an extremely Optimized Java Runtime Environment aimed at Smart phone and other device. In Mobile Platform the Security is the Challenging issue for developer. The J2ME Developer faces many challenges. The security is becoming very important issue in M-commerce. The secure Electronic Transaction and process are established through cryptographic Technologies and algorithm. Cryptographic allows us to hide information. Then it’s very important to allow cryptographic algorithm from third party toolkit to achieve Complete Security. It’s truly indeed understand reason using the third party mobile Cryptographic Toolkits.

1. Requirement of Mobile third party Toolkits are :
   
   Security:: It contains industry Standard and Certified Encryption Algorithms.

   Good Prestige: - The Mobile device becomes more general because Security provide must be good.

   Easy Deployment: - The Toolkit deploys easily in Environments that use Software Distribution Technologies.

   Overall Algorithm Support: - It should provide all effective facilities.

   2. Third Party Mobile Toolkits are :-

We are using Third Party Cryptographic Toolkits because Java Cryptographic APIs unable to provide all of these Characteristics. Following are the Some Third party Mobile Cryptographic toolkits for the developments of the M-commerce.

Bouncy Castle Toolkit: - Bouncy Castle is the Java implementation of Cryptographic Algorithm. it was developed by the Legion of the Bouncy Castle. It has made by Contribution of other packages. This Packages Contain Light Weight API that Suitable for any Environment. This Package include newly released J2ME and with additional Infrastructure.

Phaos Technology Micro Foundation Toolkit:- Phaos Technology is the Java and xml security solution Contributor. It offers toolkit for secure XML Java APIs. J2ME light weight Cryptographic APIs one of the First implementation of the SSL protocol on J2ME. the Drawback of the phaos Technology is the it can’t support the small mobile Application.

Nth Degree Truncated Polynomial Ring(NTRU) Neo for java Toolkit:- NTRU Algorithm contain NTRUEncrypt(Encryption Algorithm) and NTRU Sign(Signature Algorithm).it invented and Developed at Brown University. NTRU Provides an Implementation of its own Algorithm in Java package called as NTRU Neo for java. The Neo Encryption toolkit use fastest NTRU Cryptographic Algorithm in their c++ and java Language. It consumes least resources including CPU and battery. It’s runtime consumption below 4.5k.
B3 Security:- B3 Security Specializes in developing new lightweight Security infrastructure that minimize the present overhead related with PKI.B3 security used to assess the security of computer application and devices used within government, military and institute Organization.

From all the above Cryptographic toolkits why it’s better to use the Bouncy Castle Toolkit

- When the security error or bugs are creating, they are managed quickly.
- Bouncy Castle toolkit is flexible API Design and Community Development model. It is open Source any one contributes and discussed their own new Algorithm.
- The Bouncy Castle Community is constantly optimizing existing implementations and contributes their ideas behind concept.
- Since Bouncy Castle implements an open source JCE provider, the Bouncy castle JCE Source code use Lightweight API for multiple task.
- The Massive number of Algorithm Created in their API.

II. DESCRIPTION OF BOUNCY CASTLE

Bouncy Castle is the Third Party Cryptographic Toolkit. The Bouncy Castle Crypto APIs after Australian Charity is hand over to the Legion of the Bouncy Castle Inc. which looks after the think about and feed of the Bouncy Castle APIs.Bouncy Castle has Support many Algorithms. It has large footprint. The light weight .jar file itself has near 1MB. Most of the Mobile Application use only small subset of Bouncy Castle Algorithm.

Bouncy Castle is free license terms allow you to pack and redistribute only those classes required in your application. The Basic Package Structure of the BC package Provide its own java.math.BigInteger, java.security.SecureRandom and java.io due to the lack of support and security of such classes and packages on MIDP. The base Package that supports the Cryptographic algorithm and padding scheme is the org.bouncycastle.Crypto package [2].

The org.bouncycastle.asn1 package support the parsing and writing ASN.1 objects, which is useful in processing X.509 digital certificates [2]. The Developing an open source based pretty Good Privacy (PGP) Application; the developer can use the classes within the org.bouncycastle.bcpg package. For Mathematical support the BC use the org.bouncycastle.math.ee package.

This Mathematical provide for Elliptic Curve Cryptography. The utility classes in org.bouncycastle.util can be used for producing and reading BASE64 and hexadecimal Strings. This Utility is useful if the cipher text is required to be displayed as a Hexadecimal string [2].

Fig 1.1 Simply Package Structure of Bouncy Castle API

Fig 1.1 shows the description of various Packages that are used in Bouncy Castle API.

III. DESCRIPTION OF VARIOUS ENCRYPTION ALGORITHM

The Encryption can be divided into two parts Symmetric key (private key) and Asymmetric key (public key). In symmetric key algorithm the private key means single key can be used to encrypt and decrypt the message. Whereas in Asymmetric Algorithm used the public key and private key for encrypt and decrypt the message. However the advantage of the symmetric algorithm is that it is generally faster than Asymmetric Algorithm.

Fig 1.2 Encryption Algorithms
Symmetric Key Algorithm: - The Symmetric Algorithm used same private key. The Most commonly used technique in Symmetric Algorithm is Block Cipher and Stream Cipher. A Block Cipher is type of symmetric key Algorithm. The Block Cipher is transforming fixed length block of plaintext (unencrypted data) into Block of Cipher Text (encrypted data).

A Stream Cipher is the type of Symmetric key Algorithm. The most common used private key cipher Algorithm are DES, 3DES, AES, RC2 and RC4. Symmetric key Encryption in Bouncy Castle is Highly Flexible with the existence broad selection of cipher and cipher mode.

Asymmetric Key Algorithm: - Asymmetric key Algorithm involves the use of two Separate key are the public key and private key and the algorithm are based on the Mathematical function such as modulo and logarithmic instead of operation on bit Pattern[2]. These key mainly in three areas of application Authentication, Key Distribution and Confidentiality. However these these not all of the asymmetric algorithm can perform all these application. Mostly Elliptic Curve Cipher and RSA are more used. The RSA is public key Cryptographic algorithm it offers encryptions and digital signature (Authentication).The RSA Create their own Public and Private key. The Asymmetric Key Algorithm has occupied large Computational. And it requires large memory compare to Symmetric key Algorithm.

Password Based Encryption: - The Name Indicate of the Password Based Encryption in that password is provided by the user and generate random key based on that password. The Password Based Algorithm generates a secret key which will be provided by the end user. Password Based Encryption is typically used in system such as local encryption tools, which are used data confidentiality.

IV. CONCLUSION

In this Paper we have seen the Bouncy Castle toolkit and Key generation of different Algorithm. And also see how the Bouncy castle is better to compare other third party cryptographic toolkit. We saw key generation of symmetric algorithm and asymmetric algorithm. And various kind of other algorithm. If we used the Bouncy Castle Third party toolkit then which algorithm is better perform and support better analysis that we will see. We among discuss based on their Secure reliable performance and compare algorithm with everyone to get to know the algorithm is fast performing using Bouncy Castle toolkit. We perform to check these RC2, RC4, DES and Blowfish algorithm and check its performance. We check its efficiency, memory, speed relevant feature according to that we decide the better support algorithm. All these algorithms are belongs to symmetric key algorithm because in Asymmetric key algorithm it requires large amount memory and utilize large computational. So we decided to use symmetric algorithm to check and easily find out our result.

REFERENCES
[8] www.javawebdevelop.com