Superior Security Data Encryption Algorithm (NTRU)

Yashpal Mote, Paritosh Nehete, Shekhar Gaikwad
Guides : Ms. Sujata Tapkir, Mrs. Manjusha Yeola
M.A.E Alandi
mote.yashpal27@gmail.com, paritosh5.5cold@gmail.com,
shekhargaikwad2007@gmail.com

Abstract: *This Paper's main contribution is confidentiality, integrity and authentication in SMS (Short Message Services). The transmission of an SMS in GSMnetwork is not secure, therefore it is desirable toSecure SMS by additional encryption.In the following text, thereare various algorithmsare compared in the use of cryptography for SMS transfer securing. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks by hackers and its speed and efficiency. This paper provides aPerformance comparison between five of the most common encryption algorithms: DES, 3DES, Blowfish, AES and NTRU.The comparison has been conducted by running several encryption settings to process different sizes of data blocksto evaluate the algorithm's encryption/decryption speed. Papers main concern here is the* *performance of thesealgorithms under different conditions, the presented comparison takes into consideration the behavior and performance of the algorithm when different data loads are used. Simulation has been conducted in JAVA J2ME platform and on android O.S. At the end, this paper present a new algorithm for enhancing the performance of available algorithm. The proposed method is faster on average than the best previously known method. This paper also present a highly efficient implementation of NTRU within the android CryptographyArchitecture*

Keywords: Encryption Algorithms, Cryptography, AES, DES, TripleDES, Blowfish& NTRU.

1. Introduction

Mobile phones are part of our daily life. Nowadays, Mobile phones provide us not only communication Services, but also many multimedia and other Functionsuseful for humanbeing. Mobile phones contain private or personalData. This data is saved in a form of phone contacts,SMS, notices in a calendar, photos etc. Protection of the information depends also on a concrete user. TheUser should prevent against property of her/his with mobile phone.

If the mobile phone is in wrong hands, most of the important information is available without a great effort(Received SMS). User registers the theft of the mobile phone almost immediately, but tappingnot happens.

The SMS tapping is possible in GSM network at some places. There could be used the encryption for securing of SMS. Encryption is most often realized through some user encryption applications.

Therefore, there is a need to provide an additional encryption on the transmitted messages.

Encryption can be classified into two categories Symmetric and Asymmetric. Symmetric encryption is the process where a single key is used for both encryption and decryption. It is somehow insecure to use.

Asymmetric encryption uses two related keys, one for encryption and the other for decryption. One of the keys can be announced to the public as the publickey and another kept secret as the private key. Themajor disadvantage of symmetric encryption is the key distribution that is mostly done through a third party. Key distribution through third party can negate the essence of encryption if the key compromised by the third party.Hence, Papers study is based on the use of asymmetricencryption technique in securing SMS. There are a lot of asymmetric encryption techniques but the commonly used in the literature are Rivest, Shamir and Adleman (RSA),ELGamal3DES Advance Encryption standard (AES),Blowfish And NTRU. Due to this reason, in this study of the thementioned algorithms have been done.

This study introduces SMS, its security threats and the use of asymmetric encryption technique in securing SMS.In section 2, the related works is provided, followed by the algorithm description. Section 3 compares the underlying securityi.e. encrypt & decrypt speed of each algorithm for different packet sizes. Their performance analysis in SMS encryption is also given. Finally, Section 4 presents the conclusion of the paper.

2. Data encryption Algorithms

DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit weaknesses of DES, which made it an insecure block cipher.

3DES: As an enhancement of DES, the3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods.

AES:(Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. It was originally called

Rijndael(pronounced Rain Doll). It was selected in 1997 after a competition to select the best encryption standard. It has variable key length

of 128, 192, or 256 bits; default 256. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices Brute force attack is

The only effective attack known against it, in which the attacker tries to test all the characters combinations toun lock the encryption. Both AES and DES are block ciphers.

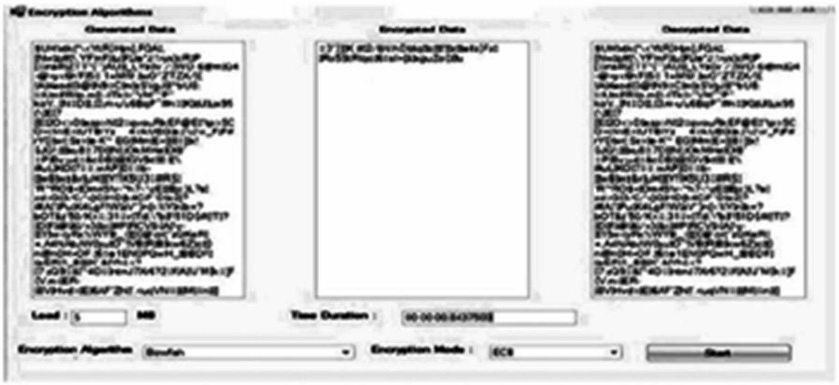
Blowfish : It is one of the most common public domainencryption algorithms provided by Bruce Schneier – oneof the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security. It takes a variable length key, ranging from 32 bits to 448bits; default 128 bits. *Blowfish is unpatented, license-free, and isavailable free for all uses.*

NTRU: The NTRU encryption scheme is an interesting alternative to well-established

Encryption schemes such as ,RSA,DES, ElGamal, and ECIES. The security of NTRU depends on the hardness of computing short lattice vectors and thus is a promising user for being quantum computer resistant. There has been extensive research onefficient implementation of the NTRU encryption scheme. In this paper, we presenta new algorithm forshowing the performance of NTRU. The proposed method is faster on average than the best previously known procedures.

3. Simulation Procedure

Here, our destination to measure the Encryption andDecryption speed for each algorithm for different packet sizes. Encryption time is used to calculate the throughput of an encryption pattern. It indicates the speed of encryption. The throughput of the encryption scheme iscalculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is decreased. By considering different sizes of data blocks (0.5MBto 20MB) the algorithms were evaluated results in terms of the time taken to encrypt and decrypt the data block. All the implementations were exact to make sure that the results will be relatively clean, fair and accurate.



Load : 5 MB

Time Duration : 00:00:00.84375

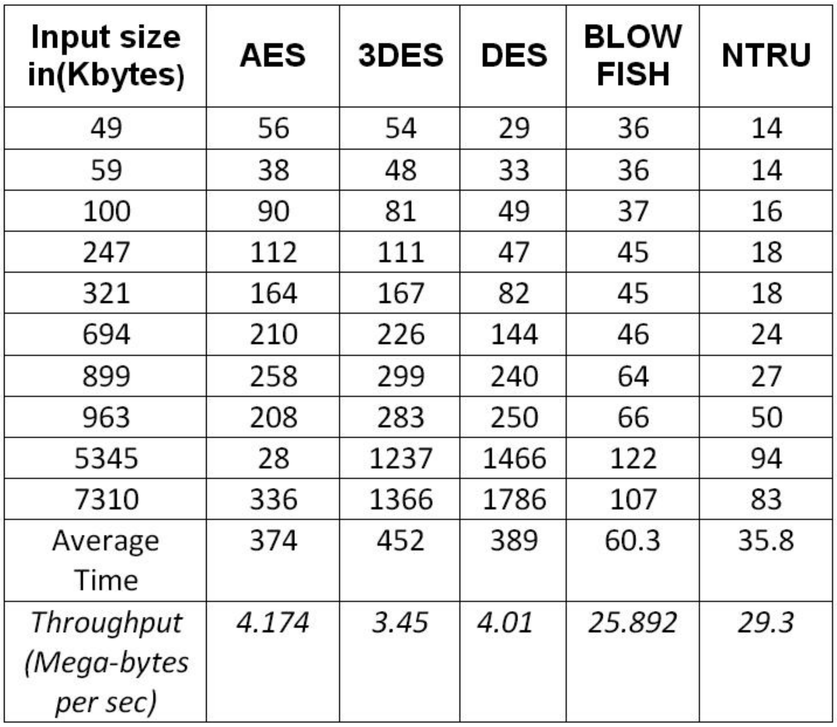
Encryption Algorithm : Blowfish

Encryption Mode : ECB

GUI of the simulation program

Figure 1- GUI of the simulation program

The Simulation program (shown in Fig. 1) Accepts Three inputs: Algorithm, Cipher Mode and data block size. After a successful execution, the data generated by it and encrypted and decrypted are shown in figure. Another comparison is made after the successful encryption/decryption process to make sure that all the data are evaluated in the right way by comparing the generated data (the originaldata blocks) and the decrypted data block generated from the process.



Input size in(Kbytes)	AES	3DES	DES	BLOW FISH	NTRU
49	56	54	29	36	14
59	38	48	33	36	14
100	90	81	49	37	16
247	112	111	47	45	18
321	164	167	82	45	18
694	210	226	144	46	24
899	258	299	240	64	27
963	208	283	250	66	50
5345	28	1237	1466	122	94
7310	336	1366	1786	107	83
Average Time	374	452	389	60.3	35.8
Throughput (Mega-bytes per sec)	*4.174*	*3.45*	*4.01*	*25.892*	*29.3*

Table 1 : Comparative Execution Times (in Milliseconds) of Encryption Algorithms with Different Packet Size.

3.1 Simulation Results

Simulation results for this compassion point are shown Fig. 2 and Table 1 at encryption stage. The results show the superiority of NTRU algorithm over other algorithms in terms of the processing time. It can also be observable here that 3DES and other algorithms has low performance in terms of power consumption and throughput when compared with DES algorithm. It requires always more time than DES because of its triple phase encryption characteristicsof it.

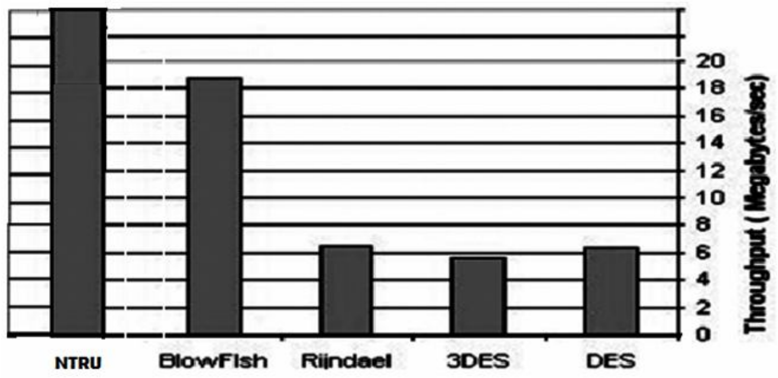


Fig. 2: Throughput of each encryption algorithm

This section will show the results obtained from running the simulation program using different data loads. The results show the impact of changing data load on each algorithm and the impact of Cipher Mode (Encryption Mode) used.

Simulation results for this compassion point are shown Fig. 3 and Table 2 decryption stage. We can find in decryption that Blowfish is the better than other algorithms and also NTRU is better than Blowfish algorithm i.e. better than all other algorithm in throughput and power consumption. So Finally,we came to know that Triple DES (3DES) still requires more time than DES algorithm.

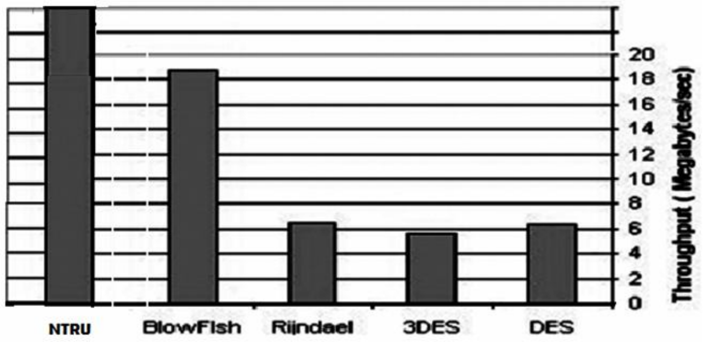


Fig. 3: Throughput of Each Decryption Algorithm (Megabyte/Sec)

3.2 Performance Results with ECB

The first set of experiments conduct observed using ECB mode, results are shown below in Figure 4.

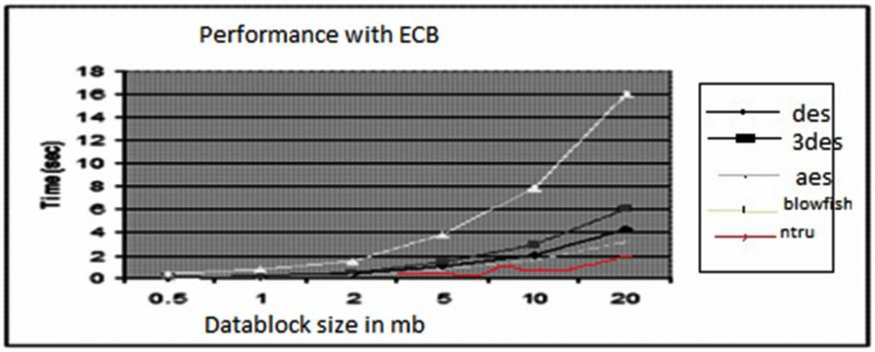
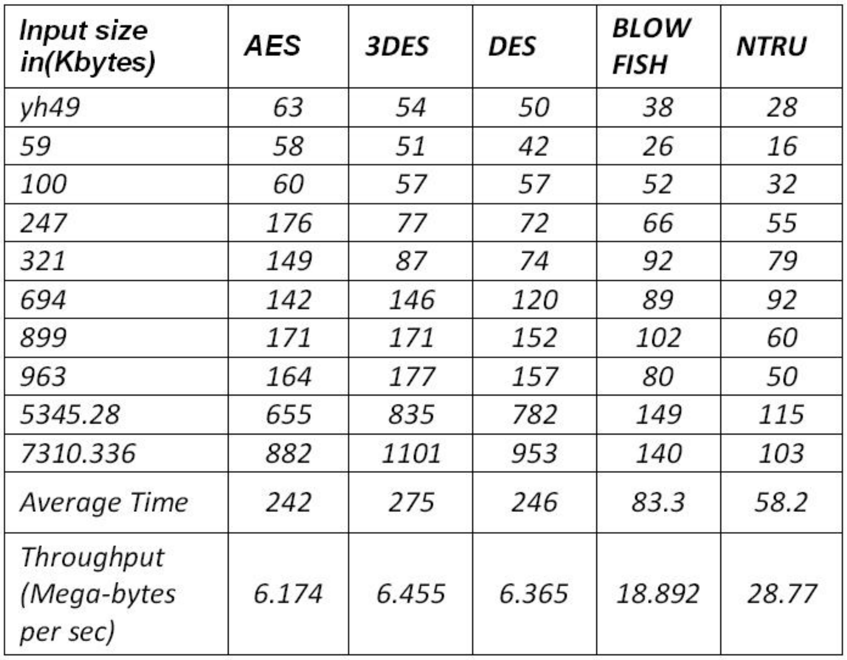


Fig. 4: Performance Results with ECB Mode

The results show the superiority of NTRUAlgorithm over all other algorithms in terms of processing time. It shows also that AESalgorithm consumes more resources when data block size is relatively big. Another point can be noticed here that 3DES algorithm requires always more time thanDES algorithm because of its triple phase encryption characteristic. NTRU, which has a long key, outperformed other encryption algorithms. DES and 3DES algorithm are known to have worm holes in their security mechanism, BlowfishAnd AES algorithms do not have any so far.



Input size in(Kbytes)	AES	3DES	DES	BLOW FISH	NTRU
yh49	63	54	50	38	28
59	58	51	42	26	16
100	60	57	57	52	32
247	176	77	72	66	55
321	149	87	74	92	79
694	142	146	120	89	92
899	171	171	152	102	60
963	164	177	157	80	50
5345.28	655	835	782	149	115
7310.336	882	1101	953	140	103
Average Time	242	275	246	83.3	58.2
Throughput (Mega-bytes per sec)	6.174	6.455	6.365	18.892	28.77

Table 2

Comparative Execution Times (in Milliseconds) of Decryption Algorithms with Different Packet Size

3.3 Performance Results with CBC

As expected, CBC requires more processing time than ECB because of its key-chaining nature of it . The results show in Fig. 5 indicates also that the extra time added is not much significant for many applications, knowing that CBC is much better than ECB in terms of the protection of the data.

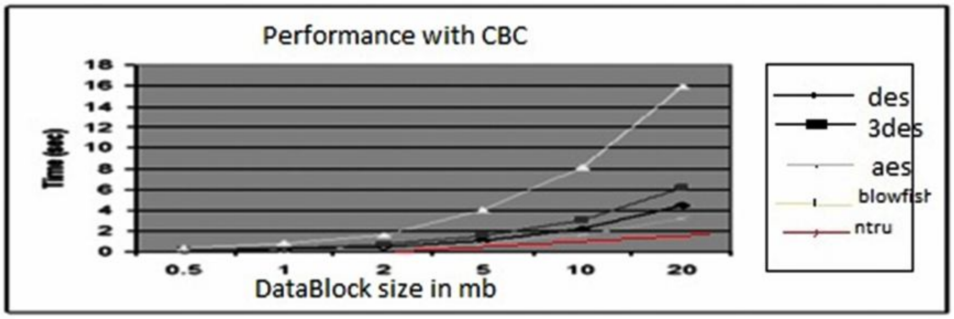


Fig. 5: Performance Results with CBC Mode

The difference between these two modes is hard to see by the naked eye, the results showed that the average difference between ECB and CBC is 0.059896 second, which is relatively very small.

4. Conclusion

The simulation results shows that NTRU algorithm has better performance than other commonly used encryption algorithms. Since NTRU has not any known security weak points so far, it can be considered as an excellent standard encryption algorithm. AES showed poor performance results compared to other algorithms, since it requires more processing power.

References

1. AamerNadeem, “A Performance Comparison of Data Encryption Algo”. IEEE 2005.

2. Ferguson, N., Schneier, B., and Kohno T., (2010). “Cryptography Engineering: Design Principles and Practical Applications”. New York : John Wiley and Sons.

3. F.I.P. Standard, Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), 2001.

4. Bruce Schneier. “The Blowfish Encryption Algorithm Retrieved”, October 25, 2008.

5. A.A. Tamimi, “‘Performance Analysis of Data Encryption Algorithms”.Retrieved October 1, 2008.

6. W. Stallings, “Cryptography and Network Security”

7. Comparison of data encryption algorithms-SimarPreet Singh, and Raman Maini

8. www.ntru.com

9. JoffreyHoffstein , Jill Pipher , Joseph H Silverman “ NTRU – A ring based public key cryptosystem”.

10. JoffreyHoffstein , Joseph H Silverman “Optimizations for NTRU”

* * * * *