Distinction between secret key and public Key cryptography with existing glitches

Aman kumar[1], Sudesh Jakhar[2], Mr. Sunil Makkar[3]

[1]M.Tech student, BRCM Bahal Bhiwani,
[2]Associate Professor, Department of Information technology, BRCM Bahal (Bhiwani),
[3]Assistant Professor, Department of Information technology, BRCM Bahal (Bhiwani).
[1]ksudesh@brcm.edu.in, [2]aman.nehra063@gmail.com.

Corresponding author: AmanKumar, Department of Information Technology, Bahal. Email: aman.nehra063@gmail.com.

Abstract

Internet use and network size is growing very fast day-by-day. So there is more need to secure the data transmitted through different services. To provide the security to the network and data different encryption methods are used. Encryption is the process of translating, plain text" unhidden" to a cipher text "hidden" to provide the security again different attacks. So as to provide the security there two wide secret and public key cryptography algorithms are used. Secret key cryptography and public key cryptography is also known as symmetrical and asymmetrical key cryptography. In this paper we will comprises the brief description of Secret key cryptography and Public key cryptography algorithms. Implement the Public Key Cryptography with RSA algorithm.

***Keywords*:** Encryption, Decryption, Plaintext, Cipher text.

1. **Introduction**.

For encryption and decryption there are two aspects: algorithm and key used for encryption and decryption. Key is similar to one time pad used in vernam cipher. If same key is used for encryption and decryption then this is called symmetric key cryptography. And if different keys are used for encryption and decryption we call this asymmetrical key cryptography (Eli Biham et al., 1990). In symmetrical key cryptography single key is used. So as before distributing the data between entities the key must be transferred. Symmetric key cryptography includes DES, AES, 3DES, Blowfish algorithms etc. and asymmetric key cryptography includes RSA, Digital Signature and Message Digest algorithms (Yogesh Kumar et al., 2011). For each algorithm there are two key aspects used: Algorithm type (define size of plain text should be encrypted per step) and algorithm mode (define cryptographic algorithm mode). Algorithm mode is combination of series of the basic algorithm and some block cipher and some feedback from previous steps.

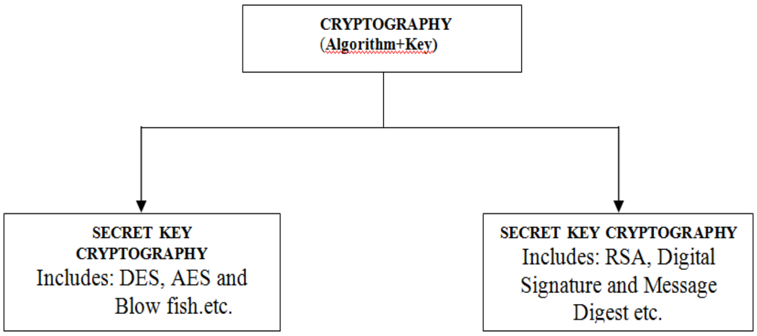

CRYPTOGRAPHY
(Algorithm+Key)
SECRET KEY CRYPTOGRAPHY
Includes: DES, AES and Blow fish.etc.
SECRET KEY CRYPTOGRAPHY
Includes: RSA, Digital Signature and Message Digest etc.

Fig.1: Cryptography types

DES—It use block cipher. It encrypts the data in block size of 8 byte each. Same algorithm and key are used for encryption and decryption. Key is 7 byte long. The position of 8, 16, 24, 32, 40, 48, 56, 64 are discarded.DES is based on two fundamental attributes of cryptography Diffusion and Confusion consisting 16 rounds. In the first round 64 bit plaintext is handed to initial permutation(IP).Then IP generates two halves left plaintext (LPT) and right plaintext (RPT). Each LPT and RPT goes through 16 rounds. At the last LPT and RPT are rejoined (Atul Kahte, 2008).

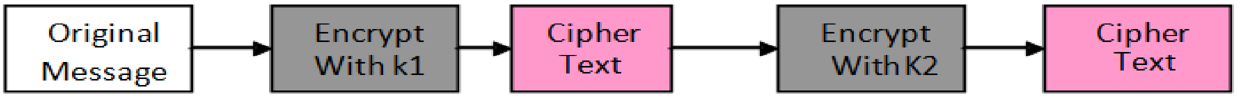


Fig. 2: Operation of 2-DES Encryption.

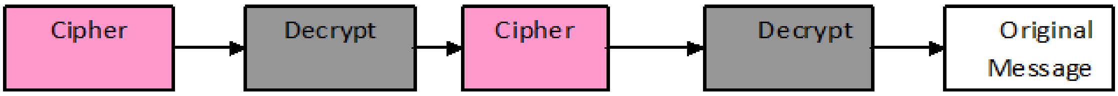


Fig.3: Operation of 2-DES Decryption

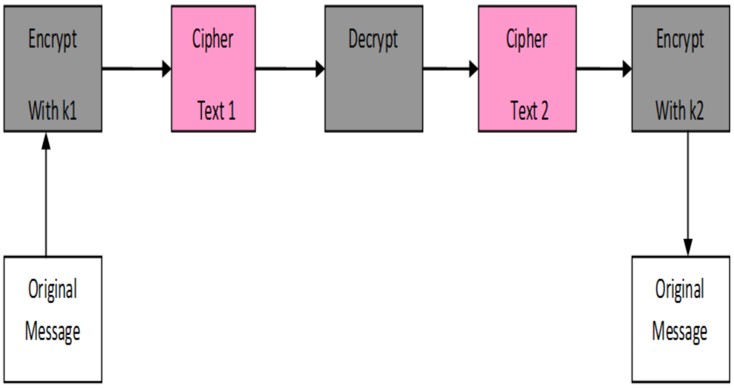


Fig.5: Operation of 3-DES with two keys (-EDE)

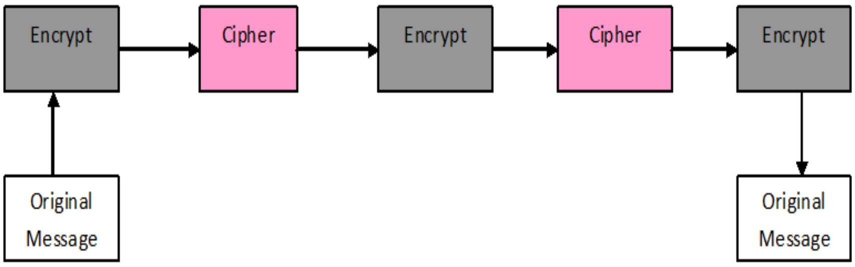
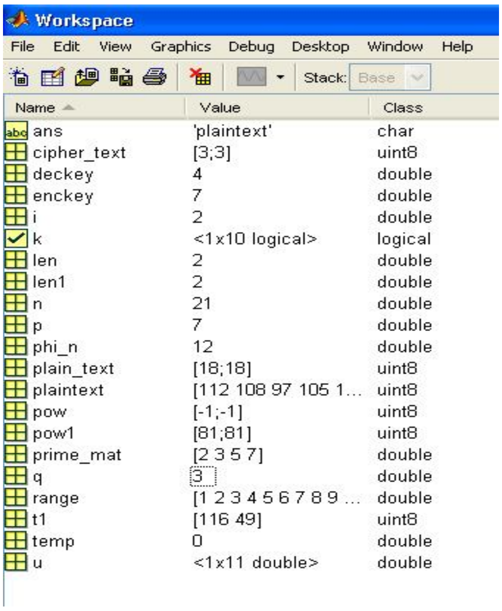
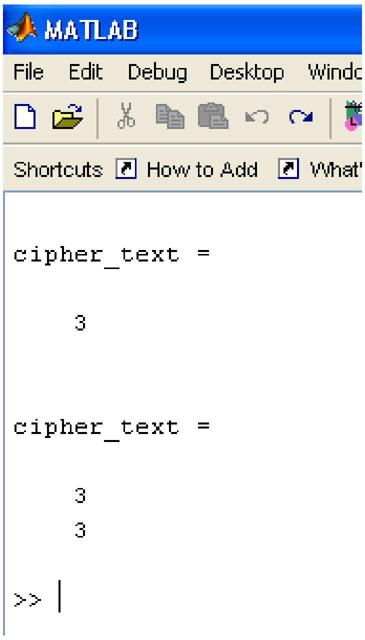


Fig.4: Operation of 3-DES with three keys (-EEE)



Name	Value	Class
ans	'plaintext'	char
cipher_text	[3;3]	uint8
deckey	4	double
enckey	7	double
i	2	double
k	<1x10 logical>	logical
len	2	double
len1	2	double
n	21	double
p	7	double
phi_n	12	double
plain_text	[18;18]	uint8
plaintext	[112 108 97 105 1...	uint8
pow	[-1;-1]	uint8
pow1	[81;81]	uint8
prime_mat	[2 3 5 7]	double
q	3	double
range	[1 2 3 4 5 6 7 8 9 ...	double
t1	[116 49]	uint8
temp	0	double
u	<1x11 double>	double

Fig.6: Work space of RSA Encryption and Decryption Operation



```
cipher_text =

     3


cipher_text =

     3
     3

>> |
```

Fig.7: Encrypted value

2DES—It performs twice same as DES normally do once. It uses two different key k1 and k2.It firstly performs the DES on the original plain text by k1 key. And then again perform encryption on encrypted text with the other key K2 shown in (Fig. 2) and decryption is shown in (Fig. 3).

3DES— It was enhancement of DES. And used to remove the mid-in-the-middle attack occurred in 2-DES. In this 3 times iterations of DES encryption on each block is performed as shown in fig.4 & 5. In 3-DES the 3-times iteration is applied to increase the encryption level and average time. Common method of 3-DES is Minus Encrypt-Decrypt-Encrypt (-EDE). Each iteration of 3DES using –EDE will encrypt a block using a 56-bit key shown in (Fig. 4). After encryption, use a different 56-bit key to decrypt the block. On the last pass, a 56-bit key is used to encrypt the data again. This is equivalent to using a 168-bit encryption key. Another method that is Minus Encryption- Encryption – Encryption (-EEE) shown in (Fig. 5). All three keys can be different or identical or first and third key can be same (Atul Kahte, 2008).

AES— It use block cipher. It encrypts the data in block size of 128 bits each. Same algorithm and key are used for encryption and decryption. It uses variable key length of 16, 24 or 32 bytes key length using 9, 11 and 13 processing rounds to perform encryption. The main features of AES are its symmetrical and parallel structure, adapted to modern processor and suited for smart cards.AES is fast and flexible *(*Yogesh Kumar et al., 2011*)*.

We have studied a no. of different techniques used for fulfillment of data encryption purpose. So there are some comparisons generated on different important features.

- *Avalanche effect*: - Small change in plaintext or key will change the cipher text is Known as advance effect. Either change in on bit of plaintext or key will change no. bits of output value.

- *Memory required*:-Different algorithm required different memory space to perform the operation. The memory space required by any algorithm is determined on the basis of data size, no. of rounds etc.From different algorithm an algorithm is considered best which use small memory and perform best task.

- *Simulation time:* The time required consumed by algorithm to complete the operation is known as simulation time. It depends on processor speed, algorithm complexity. Small simulation time is desirable requirement *(*Himani Agarwal et al., 2010*)*

2. Description of Public key cryptographic Algorithm along with existing glitches.

2.1 RSA Algorithm

This is public key encryption algorithm developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is most popular and asymmetric key cryptographic algorithm. It may used to provide both secrecy and digital signature. It uses the prime no. to generate the public and private key based on mathematical fact and multiplying large numbers together. It uses the block size data in which plaintext and cipher text are integers between 0and n1 for some n values. Size of n is considered 1024bits or 309 decimal digits. In this two different keys are used for encryption and decryption purpose. As sender knows encryption key and receiver knows decryption key.

Table 1: Comparison between Secret Key Cryptography and Public Key Cryptography

Features	Secret Key Cryptography	Public Key Cryptography
Key Used	Same key is used for encryption and decryption purpose.	Different keys are used for encryption and decryption purpose.
Speed	Very fast	Slow
Key Agreement / Distribution	To agree on the same key by sender and receiver is the biggest problem	No key agreement is needed.
Scalability	It is scalable algorithm due to varying the key size and block size.	No scalability occurs.
Factorization Problem	No factorization is required to select the key.	To select the key select the from prime numbers factorization is performed i.e. RSA
Avalanche Effect	No more effected	More effected
Memory Used	Large	Small
Processing Speed	Very High	Slow
Confidentiality	High	Low

Following steps are followed in RSA to generate the public and private keys:
Choose large prime numbers p and q such that p~=q.
Compute n=p*q
Compute φ (pq) = (p-1)*(q-1)
Choose the public key e such that gcd (φ (n), e) =1; 1<e< φ (n)
Select the private key d such that d*e mod φ (n) =1
So in RSA algorithm encryption and decryption are performed as-
Encryption

Calculate cipher text C from plaintext message M such that
C=M ^e mod n
Decryption
M=C^d mod n=M^ed mod n
2.2 Glitches in RSA algorithm:

- Integer factorization problem occurred.
- RSA use different keys for encryption and decryption purpose. So it is difficult to choose these keys randomly.
- The speed of encryption in public key cryptography algorithm is slow as it used 8bit block size data.
- RSA private key is not secure.
  As (p-1) for p is one of the factors of n is product of small prime numbers.
- Difficult to factorize a large no. to provide security in this.

3. Comparison

Comparison of secret key and public key cryptography. Public key cryptography solves the problem of the key agreement and key exchange problem generated in secret key cryptography .But it does not solve all the security infrastructure .So secret key and public key cryptography differs from each other in certain features. Both have areas where one is best suited but another is not or vice-versa mentioned in (Table.1).

4. Conclusion

This paper presents a theoretical performance of selected public key and secret key cryptography algorithm. The selected algorithms are DES and RSA with their working mechanisms. As in the public key cryptography the key distribution and key agreement is the highest priority .There is no doubt that public key cryptography system provide high security. As this paper also results that public key cryptography is used where the secret key is not suited best or vice-versa.

References

1. Atul Kahte (2008) Cryptography and Network Security, 2nd Ed.
2. Dan Boneh and Glenn Durfee (1999) Cryptanalysis of low exponent RSA
3. Diffie W, Hellman ME (1976) New Directions in cryptography.
4. Eli Biham & Adli Shamir (1990) Differential Cryptanalysis of full DES.
5. Ferguson N, Schnier B & Konho T (2010) Cryptography Engineering: Design principles and Practical applications, 1st Ed.
6. Himani Agarwal & Manish Sharma (2010) Implementation and analysis of various symmetric cryptosystems, Indian Journal of Science and Technology, 3(11) Dec-2010.
7. Piper F (1997) Encryption. Security and Detection, Ecos. European Conference.
8. Schweighofer E (1997) Downloading information Information & Communication technology.
9. Yogesh Kumar, Rajiv Munjal (2011) Comparision of symmetric and asymmetric cryptography with existing Vulnerabilities IJCMS.