INFORMATION SECURITY USING BLOWFISH ALGORITHM IN E-BANKING

Anupam Baruah¹, Prof.(Dr.)Lakshmi Prasad Saikia²
¹Research Scholar, Dept. of Computer Science & Engineering, Assam down town University, India
²Professor, Dept. of Computer Science & Engineering, Assam down town University, India
¹anupambaruah04@gmail.com; ²lp_saikia@yahoo.co.in

Abstract— E-Banking provides all banking services to its users over the internet. Some of the services include paying of bills, Fund transfer, transfer, viewing account statement, etc. Users can easily access their e-banking account through internet via computers and Smartphone using wi-fi or 3g/4g connection. But security of fund transaction is a very big issue. There is a possibility to hack user’s account information by hackers at any time over internet. Cryptography is a best technique for encrypt data from outside Hackers. In this paper we implement a banking system by using Blowfish algorithm. This system will provide a secure web base application where only authorize users can access all information using a valid secret key.

Keywords— Cryptography, Symmetric key encryption, Asymmetric key encryption, Blowfish algorithm

I. INTRODUCTION

In modern era, Internet Banking plays an important roll of our daily life. E-banking means services provided by the banks over internet. Some services include fund transfer, bill payment, and view account statement online. Users can do all services at any time because there is no global time for internet. But we should keep our important information from hackers. So data encryption is an important part in this system. Cryptography provides the necessary tools for accomplishing secure and authenticated transactions[1]. There are many cryptographic algorithms like RSA encryption algorithm, DSA encryption algorithm, Blowfish algorithm, two fish algorithm, AES algorithm etc. In the system implementation we are using Blowfish algorithm as encryption techniques which is a symmetric key block cipher design.

MEANING OF CRYPTOGRAPHY:

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. It deals with the actual securing of digital data. The primary objective of using cryptography is to provide the four fundamental services i.e.
a) **Confidentiality**: It is a security service that keeps the information from an unauthorized person. It is also referred to as privacy or secrecy.
b) **Data integrity**: It deals with the identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently.
c) **Authentication**: It provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.
d) **Non-repudiation**: It is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

**SYMMETRIC KEY ENCRYPTION**
The encryption process where same keys are used for encrypting and decrypting the information is known as symmetric key encryption. The study of symmetric cryptosystem is referred to as symmetric key cryptography.

**ASYMMETRIC KEY ENCRYPTION**
In asymmetric key encryption different keys are used for encrypting and decrypting the information. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible.
Blowfish
In 1993, Bruce Schneier designed Blowfish algorithm. The elementary operators of Blowfish algorithm include table lookup, addition and XOR. Blowfish is a 64bit block cipher and can encrypt data on 32-bit microprocessors. It can also run in less than 5k of memory. It uses addition, XOR, lookup table with 32-bit operand [2]. The algorithm consists of two parts: a key-expansion part and a data-encryption part. Key expansion converts a key of at most 448 bits into several subkey arrays totalling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words.

II. RELATED WORK
In 2010, Diaa Salama Abd Elminaam, Hatem Mohamed Abdul Kader and Mohiy Mohamed Hadhoud evaluated the performance of Symmetric Encryption Algorithms. They used some selected algorithms which are AES, DES, 3DES, RCC, BLOWFISH in their model [1].

In 2013, Tanjyot Aurora and Parul Arora implemented a secret key block cipher algorithm “Blowfish algorithm” from the prospective cryptology. They made a design and implementation of Blowfish algorithm by which client can manage their userid and password efficiently. An Implementation of Feistel network for encryption files is also examined in their work [2].

In 2014, Mrs Veena Jose and Ms. C. Divya implemented Blowfish algorithm for secure data transmission. The data to be transmitted is stored in a file and the file is encrypted using Blowfish algorithm. This encrypted file is communicated among the group members, such that they can easily decrypt the file using same key which is known to them [3].

In 2014, Ms Neha Khatri and Prof. V. K Kshirsagar introduced an algorithm works on the same line as DES and it consumes block coding with blocks of a size of 64 bit. Blowfish became quite popular after its advent. The proposed algorithm of the Blowfish can achieve efficient data encryption up to 4 bits per clock [4].

In 2015, Saikumar mankan and K vasanth introduced an algorithm for information security is designed and analysed. The work is done for networking and communication applications for enhanced network security and defence applications. They presented simulation result that shows encryption and decryption process using Blowfish algorithm [5].

III. METHODOLOGY

A. Customer registration process:
In my system both admin and stuff can add customer. After inserting all details of customer an account number and a secret key will generate against each customer. Every customer must remember his/her secret key. At the time of registration all customer’s data are converted to cipher text by blowfish algorithm with a key. Same key must be used to decrypt the cipher text to plain text.
**Encryption process:**

![Fig 3.1](image)

In this encryption process, some data like account number, phone number, secret key, date of birth etc of each customer are encrypted by blowfish algorithm with an encryption key.

![Fig 3.2](image)

After successful login customer have to insert secret key to decrypt all encrypted text. Here the same key uses to decrypt the text.

The basic algorithm for Blowfish algorithm is illustrated as follows.

Divide x into two 32-bit halves: xL, xR

For i = 1 to 16:

- \( xL = xL \oplus P_i \)
- \( xR = F(xL) \oplus xR \)
- Swap XL and xR
- Swap XL and xR (Undo the last swap.)
- \( xR = xR \oplus P_{17} \)
- \( xL = xL \oplus P_{18} \)
Recombine xL and xR
Output 64 bit X(Cipher text).

IV. SIMULATION AND RESULT
In this paper, we have simulated Encryption and decryption part in PHP language. There are mainly three (3) sections like admin section, stuff and customer. Admin can do all operations including creation of customer and stuff, updating of customer and stuff details, deletion of stuff and customer details etc. Stuff only can create customer and also can update customer’s details. Customers can view their account details, can transfer fund, can add beneficiary details, etc.

Fig 4.1: Admin login area

Admin can login using emailed and password. After successful login page redirects to admin dashboard.

Fig 4.2: Admin Dashboard
Admin can view, edit, and delete stuff/customers. There is a change password link where admin can update his/her password.

**Fig 4.3: Generate secret key**

In customer registration form, admin can add customers to the system. He can edit or delete customers also.

**Fig 4.4: Customer registration**
Fig 4.5: Customer login area

Customer can login to the system using customer user-id and password. After successful login page redirect to customer dashboard page where customers can view their profile, can add beneficiary, can transfer funds etc.

Fig 4.6: Customer dashboard with encrypted balance and account number

In customer dashboard area account number and total balance is encrypted using blowfish algorithm. Customers must enter secret key to decrypt the cipher text.
Fig 4.7: Customer dashboard with decrypted balance and account number

Total balance and account number is converted to human readable plain text after putting the secret key to the input field.

V. CONCLUSION

In modern communication system, Information security plays an important role. All confidential or important information send on internet, so it is very important to keep records secure. So to protect our information, we should take importance in Privacy, integrity, confidentiality and non repudiation. When customer transfers money to any beneficiary over internet the protection of data against security threats is a major issue. During transaction the data must be protected from unauthorized access. In our system, we have used blowfish algorithm. The algorithm encrypts information to unreadable format and then sends over internet which increases the level of security dimensions.

REFERENCES