Bit Rotation

SNAPPER CRYPTOGRAPHY ALGORITHM

Sandeep kella
(Lead cryptographer)

Snapper Technologies
Fintech Tower Vizag 2nd Floor,
Sunrise Incubation Hub
Hill No 2, Plot No 13 & 14
Madhurawada, Rushikonda
Visakhapatnam – 530045

www.snappertech.com

Summary

In an age of explosive worldwide growth of electronic data storage and communications, many vital national interests require the effective protection of information. When used in conjunction with other approaches to information security, cryptography is a very powerful tool for protecting information. Consequently, current Indian policy should be changed to promote and encourage the widespread use of cryptography for the protection of the information interests of individuals, businesses, government agencies, and the nation as a whole, while respecting legitimate national needs of law enforcement and intelligence for national security and foreign policy purposes to the extent consistent with good information protection.

Problems in current Eco-system

The increase in new cyber threats has made it difficult for the existing cyber security products to cope up with the upcoming malwares and ransomwares

e.g WannaCry attack in May 2017.

Goals

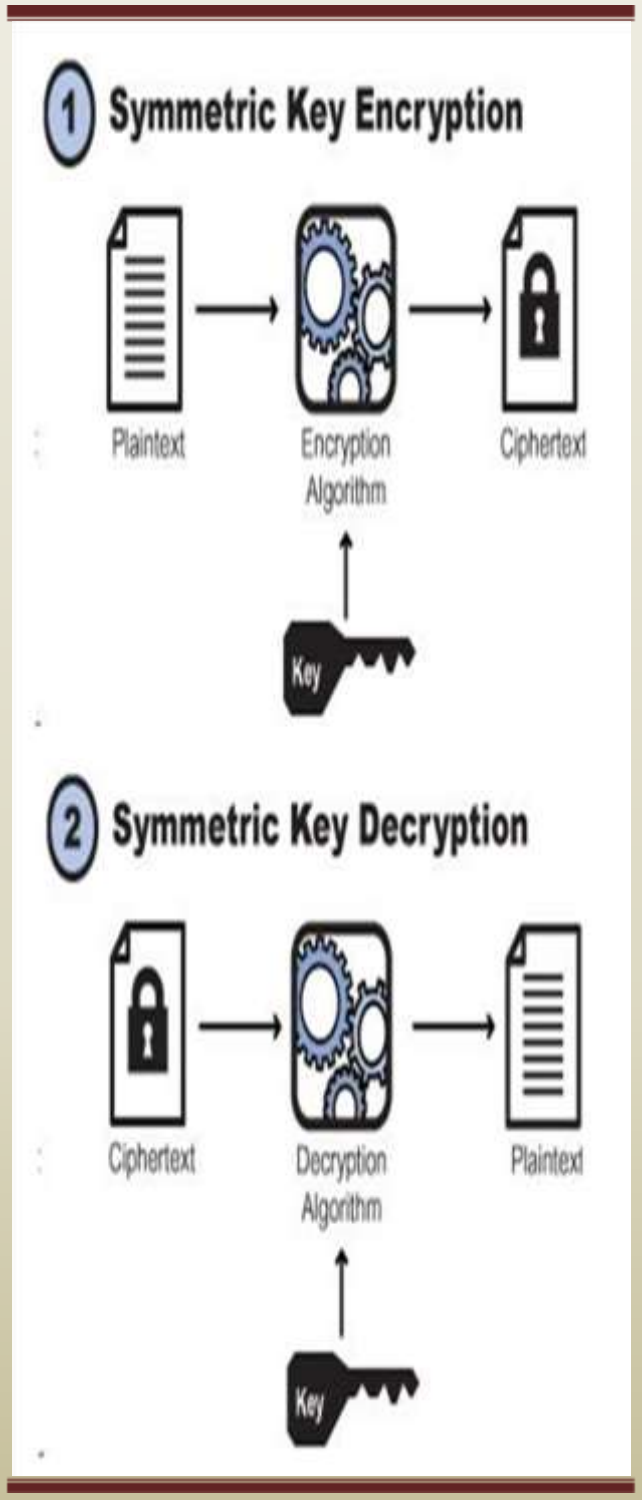
The goal of the cryptography is to protect private communication in the public world. The assumption is that two entities wanting to communicate - Alice and Bob - are shouting their messages in a room full of people. Everyone can hear what they are saying. The goal of cryptography is to protect this communication so that only Alice and Bob can understand the content of the messages.

Introduction to Cryptography

The Indian economy fundamentally changed in the last twenty years, as Service and IT sectors dominating traditional manufacturing and agricultural sector, there is a need to focus on knowledge and data. This transformation has underscored the importance of safeguarding information through encryption. This article focuses on state-of-the-art encryption techniques used pervasively to protect data, such as personal identity, medical records, financial transactions, and electronic mail, to name a few.

A typical approach to security is to strike a balance between apparent risks to information and efforts to mitigate those risks. A common standard used to determine the level of security required is "commercial impracticability" - if it takes longer to access critical data than the timeframe within which its knowledge confers some benefit, practical security has been achieved. For example, if your credit card information is protected by a system that would take the most sophisticated hacker five years to unlock, but you obtain new credit card numbers every two years on average, there will be little benefit to 'breaking' the security scheme.

An important concept in security is that virtually any security system can and will be compromised eventually; it simply takes time. For example, the Japanese never broke the code employed with great success by the Navajo code talkers in the Pacific theatre during World War II, but their code was only employed for a few years. The success of that code was the use of words in a foreign and little-known language to represent military messages. Had the Japanese efforts to decrypt the Navajo code focused more on linguistics than cryptography, it would have likely been just another broken security scheme in a long line of others.



Encryption

Encryption algorithms or ciphers are mathematical formulas or functions applied to data to transform the unprotected information, or plaintext or cleartext, into an unrecognizable format commonly referred to as **ciphertext**.

There are generally two inputs to an encryption algorithm: a **key** and the **plaintext** itself. In some cases the ciphertext is larger than its associated plaintext or the same size. The goal is to make the time it would take to recover or decipher the plaintext, having only the ciphertext and not the key, so long as to greatly exceed the time-value of the plaintext. Ideally, a strong algorithm and key combination should take at least millions of years to break, based on mathematical predictions.

Decryption

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term

could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general protection of company data and trade secrets. If this data needs to be viewable, it may require decryption. If a decryption passcode or key is not available, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable.

Here are some commonly used algorithms:

DES/3DES or TripleDES
This is an encryption algorithm called Data Encryption Standard that was first used by the U.S. Government in the late 70's. It is commonly used in ATM machines (to encrypt PINs) and is utilized in UNIX password encryption. Triple DES or 3DES has replaced the older versions as a more secure method of encryption, as it encrypts data three times and uses a different key for at least one of the versions.

Blowfish
Blowfish is a symmetric block cipher that is unpatented and free to use. It was developed by Bruce Schneier and introduced in 1993.

AES
Advanced Encryption Standard or Rijndael; it uses the Rijndael block cipher approved by the National Institute of Standards and Technology (NIST). AES was originated by cryptographers Joan Daemen and Vincent Rijmen and replaced DES as the U.S. Government encryption technique in 2000.

Twofish
Twofish is a block cipher designed by Counterpane Labs. It was one of the five Advanced Encryption Standard (AES) finalists and is unpatented and open source.

IDEA
This encryption algorithm was used in Pretty Good Privacy (PGP) Version 2 and is an optional algorithm in OpenPGP. IDEA features 64–bit blocks with a 128–bit key.

MD5
MD5 was developed by Professor Ronald Riverst and was used to create digital signatures. It is a one–way hash function and intended for 32–bit machines. It replaced the MD4 algorithm.

SHA–1
SHA–1 is a hashing algorithm similar to MD5, yet SHA–1 may replace MD5 since it offers more security

HMAC
This is a hashing method similar to MD5 and SHA–1, sometimes referred to as HMAC–MD5 and HMAC–SHA1.

RSA Security
RC4– RC4 is a variable key–size stream cipher based on the use of a random permutation.
RC5– This is a parameterized algorithm with a variable block, key size and number of rounds.
RC6– This an evolution of RC5, it is also a parameterized algorithm that has variable block, key and a number of rounds. This algorithm has integer multiplication and 4–bit working registers.

Current threats in the Eco-system

WannaCry ransomware attack

The WannaCry ransomeware attack is an ongoing worldwide cyberattack by the WannaCry ransomware cryptoworm (also known as WannaCrypt.) which targets computers running the Microsoft Windows operating system, encryption data and demanding ransom payments in Bitcoin Cryptocurrency.

The attack started on Friday, 12 May 2017 and has been described as unprecedented in scale, infecting more than 230,000 computers in over 150 countries. The worst-hit countries are reported to be Russia, Ukraine, India and Taiwan but parts of Britain's National Health Service (NHS), Spain's Telefonica, FedEx, Deutsche Bahn, and LATAM Airlines were hit along with many others countries & companies worldwide.

Indian Debit Card Hack

Who? Unknown

What? As many as 32 lakh debit cards belonging to various Indian banks were compromised earlier, 2016 resulting in the loss of Rs 1.3 crore in fraudulent transactions as per NPCI.

Bangladesh Bank Hacks

Who? Unknown

What? One of the largest financial crimes executed online took place in early February when $81 million of Bangladesh's money was siphoned off by unknown hackers, reportedly to Philippines, Sri Lanka and parts of Asia.

Existing algorithms

DES/3DES or TripleDES, Blowfish , AES, Twofish, IDEA, RSA Security

Our Product

For every algothims the inputs are plain text and key and the output is encrypted text .

But here for every algorthim there is and unique encrypted text for every plain text and key.

Plain text + key = encrypted text

Abc + 12 = xyz

Abc + 12 = xyz

Abc + 12 = xyz

.

.

……..

In bit rotation algorthim there will different encrypted text for same plain , key

Abc + 12 = xyz

Abc + 12 = lmn

Abc + 12 = wer

.

.

……..

```
E:\programs\rotate\bit matix>java encrypt
 enter text
abc
  enter key 4
^W[@~

E:\programs\rotate\bit matix>java encrypt
 enter text
abc
  enter key 4
UGVUd

E:\programs\rotate\bit matix>java encrypt
 enter text
abc
  enter key 4
bYEctD
```

Bit rotation algorithm does not use any formula for encryption

```
E:\programs\rotate\bit matix>java decrypt
 enter encrypted text ^W[^F@~
 enter key 4

 output =abc
E:\programs\rotate\bit matix>java decrypt
 enter encrypted text U^VGVUd
 enter key 4

 output =abc
E:\programs\rotate\bit matix>java decrypt
 enter encrypted text bYEctD
 enter key 4

 output =abc
```

Cryptography – Benefits

Cryptography is an essential information security tool. It provides the four most basic services of information security −

- **Confidentiality** − Encryption technique can guard the information and communication from unauthorized revelation and access of information.
- **Authentication** − The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- **Data Integrity** − The cryptographic hash functions are playing vital role in assuring the users about the data integrity.
- **Non-repudiation** − The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

All these fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

Conclusion

The importance of computers and networks and the information they store and communicate to society today are equalled only by the threats to them.

The recent WannaCry, which has infected thousands of computer systems in 150 countries, is a frightening reminder of the vulnerabilities of a connected world.

The encryption algorithms discussed in this article are in many instances the only protection between our critical information and those who seek to compromise and exploit it.