Mphasis
The Next Applied

CRYPTOGRAPHY
Enlightening its importance on Network Security

Whitepaper by
SRUTHY VISWANATH
Delivery Associate Software Engineer

Abstract

Using various means of communication over the internet, such as electronic mail, or making purchases from online stores/websites are not considered as secured means of sending and receiving information. Information sent by those means includes sensitive personal data which may be intercepted by intruders. Hence, in order to perform these activities in a safe manner, users would like to have a secure, private communication with the third-party. Cryptographic algorithms are thus introduced to keep our information secured from prying eyes; these algorithms encode the message in a way that no one other than its intended recipient can read it.

Introduction

Cryptography is a method of storing and transmitting data in a way that only the intended recipient can read and process it. More generally, cryptography is about constructing and examining protocols that prevent third-parties or public from reading private messages so that they do not disrupt in any aspect of information security, such as data integrity, data confidentiality, authentication, and non-repudiation.

Components

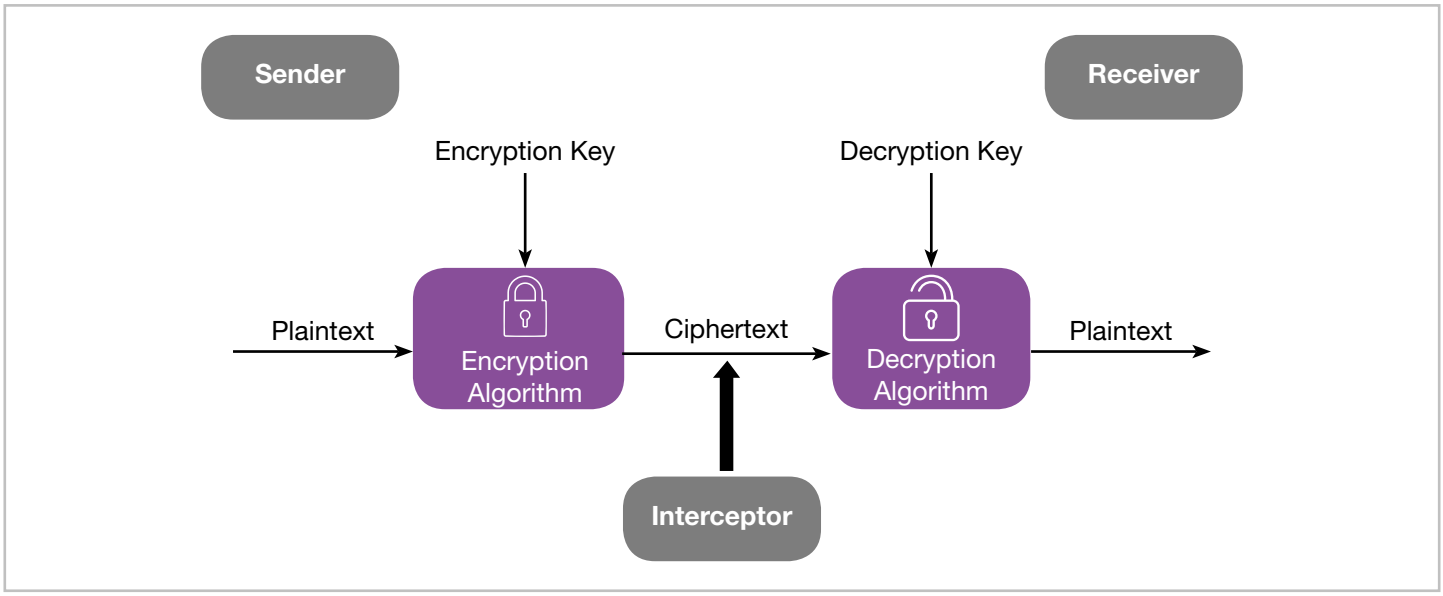


Fig. 1

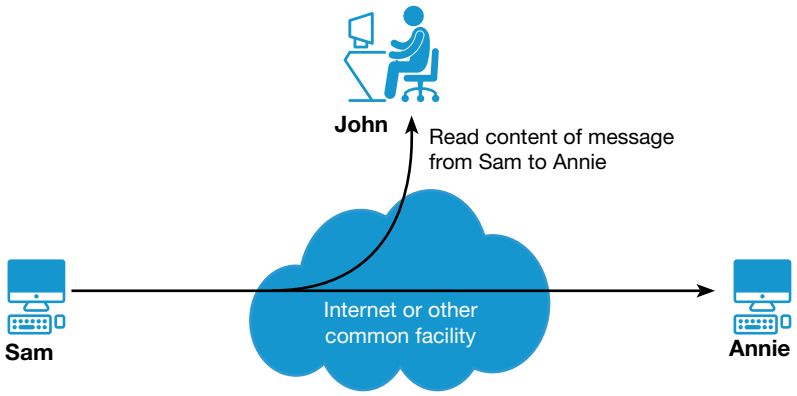
The outgoing message is encrypted before transmission using Encryption Algorithm. This algorithm that takes plaintext and an encryption key as input, produces a ciphertext. The transformation makes the message hard to read, and hence secured. If someone wants to read it, he/she must decrypt it using Decryption Algorithm, which produces a unique plaintext for any given ciphertext. and decryption key. Only the two parties – sending as well as receiving – should have access to the confidential information around the key and the algorithm used.

Attacks on Cryptosystems

Attacks are usually classified based on the action performed by the attacker. An attack can be **passive** or **active.**

Passive Attacks

The main aim of a passive attack is to obtain access to information in illegal way. For example, actions such as intercepting and intruding the communication channel. These are passive in nature as they do not affect the information or disrupt the communication channel. A passive attack is usually seen as stealing the information. The only difference in stealing goods and stealing information is that when data is stolen it still leaves the owner in possession of that data. Hence, passive attack is more dangerous than stealing of goods, as information leaked may go unnoticed by the owner.



Release of message contents (Passive Attacks)

Fig. 2

Active Attacks

An active attack involves **changing the information** by processing it in some way. For example an attacker can:

- Modify the intercepted information
- Initiate unintended or unauthorized transmission of information
- Alter the authenticated data
- Deny the access to information for legitimate users (denial of service)

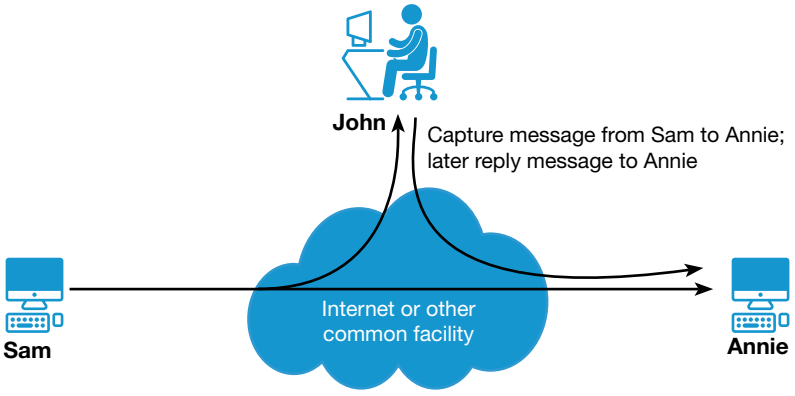


Fig. 3

Types of Cryptosystems

Symmetric

Symmetric key cryptography or secret key cryptosystems is an encryption method where same key is used by sender as well as receiver (or, in other words, it is an encryption method where keys are different but are related in an easily computable way).

Symmetric key ciphers are executed as either block ciphers or stream ciphers. A block cipher encrypts the data in blocks of plaintext as opposed the input form used by a stream cipher. Stream ciphers, as opposed to the block type, create a stream of key material that is then combined with the plaintext bit-by-bit or character-by-character.

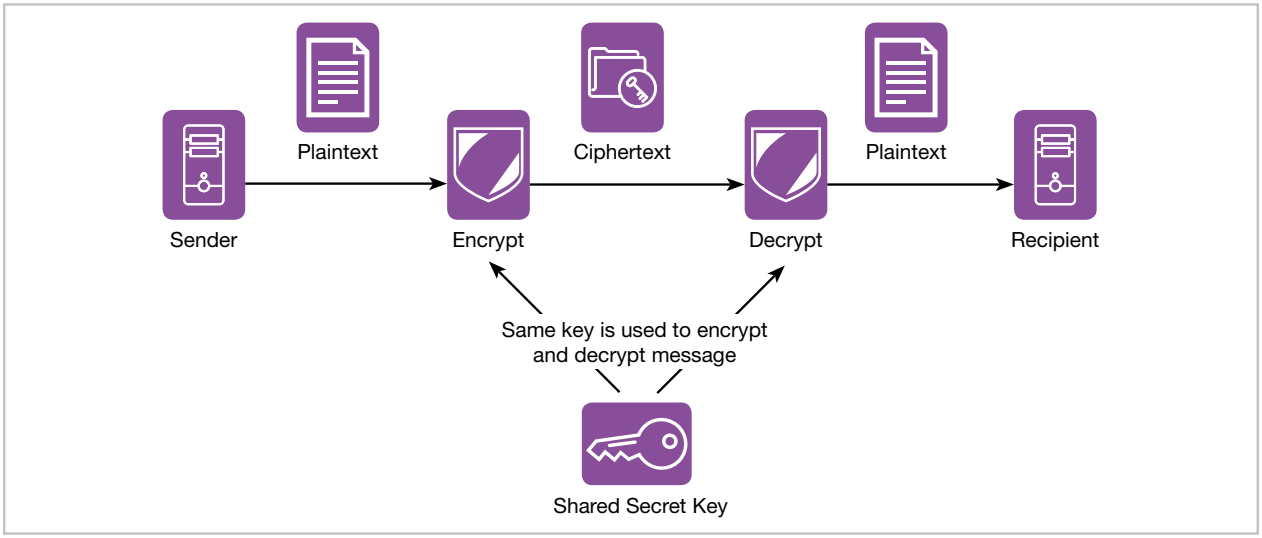


Fig. 4

Challenges of Symmetric Key Cryptosystem

There are two restrictive challenges of using symmetric key cryptography:

- **Key establishment** – Before start of any communication the sender and receiver should agree on same symmetric key which requires a secure key establishment mechanism in place
- **Trust issue** – Both the communicating parties are required to trust each other, by default, as same symmetric key is being used

Asymmetric

The main disadvantage of symmetric key cryptography is the trust issue while agreeing on a same key by both the communicating parties. As a solution to that, both communicating parties must exchange different keys as well as ciphertext.

Whitfield Diffie and Martin Hellman proposed the concept of **public key**, also known as **asymmetric key cryptography**, in which two completely different, however mathematically related, keys - **a public key** and **a private key** were generated. Calculating one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are related to a certain extent. Instead, both keys are generated secretly, as an interrelated pair.

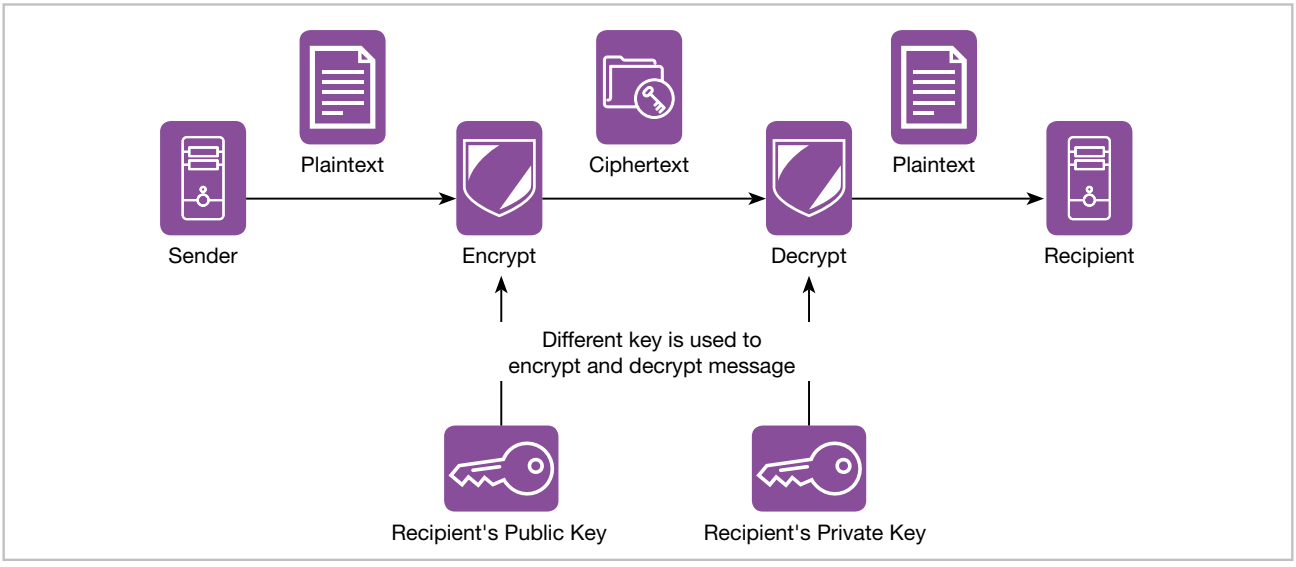


Fig. 5

Challenges of Public Key Cryptosystem

Public key cryptosystems have one significant challenge – trust issue. The user should trust that public key he is using in communications is the public key of that person and has not been hoaxed by a mischievous third-party.

This issue is taken care by a Public Key Infrastructure (PKI) comprising a trusted third-party. This party manages and attests that public keys are being generated from legal source. When the third-party is asked to provide the public key for any communicating person X, they are believed to provide the correct public key.

Popularly used Encryption Technologies

Earlier Caesar cipher used to be the most famous one, which was used by the military commanders of the Roman emperor Julius Caesar. Each letter of the encrypted text (the ciphertext) in the message was replaced by another letter some fixed number of places down the alphabet. But over time such simple methods have proved to be insecure as eavesdroppers, called cryptanalysts, could recover plaintext and even the decryption key from ciphertext through some easy mathematical computation, allowing them to easily decipher any future messages from that system.

Modern computing technology has made it practical to use more complicated encryption algorithms that are harder to break by cryptanalysts. In parallel, cryptanalysts have acquired and developed the technology to improve their ability to break cryptosystems.

There are various types of encryption algorithms available with different key size and strength -

Triple DES

DES (Data Encryption Standard) was once the most commonly used algorithm for encrypting data in industry. This encryption algorithm is implemented to take a fixed-length of plaintext and convert it into ciphertext after conducting 16 rounds of operations. The DES algorithm takes a single 56-bit key and uses it on the data queued for encryption in 64-bit data blocks. The resulting text after transformation is the same length as the input text. In addition to this, the DES key is also 64-bit in length, however, 56-bit are used by the algorithm and the remaining 8-bit are used for parity checking. These 8-bit are then discarded making the actual key length 56-bit. Today, DES is not considered to be too safe for a number of transactions due to the fact that 56-bit key size is too small for modern technology.

Triple DES was implemented to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat easily. Triple DES was once the recommended standard and the most extensively used symmetric algorithm in the industry.

Triple DES uses **three independent keys with 56-bit each**. The total key length sums up to 168-bit, but experts would argue that 112-bit in key strength is more like it. First, encrypt the plaintext blocks using single DES with key 1. Now decrypt this output using single DES with key 2. Finally, again, encrypt using single DES with key 3. The final output is the ciphertext. Decryption process is exactly the opposite.

In spite of slowly being phased out, Triple DES still manages to make a dependable hardware encryption technique for financial services and other industries.

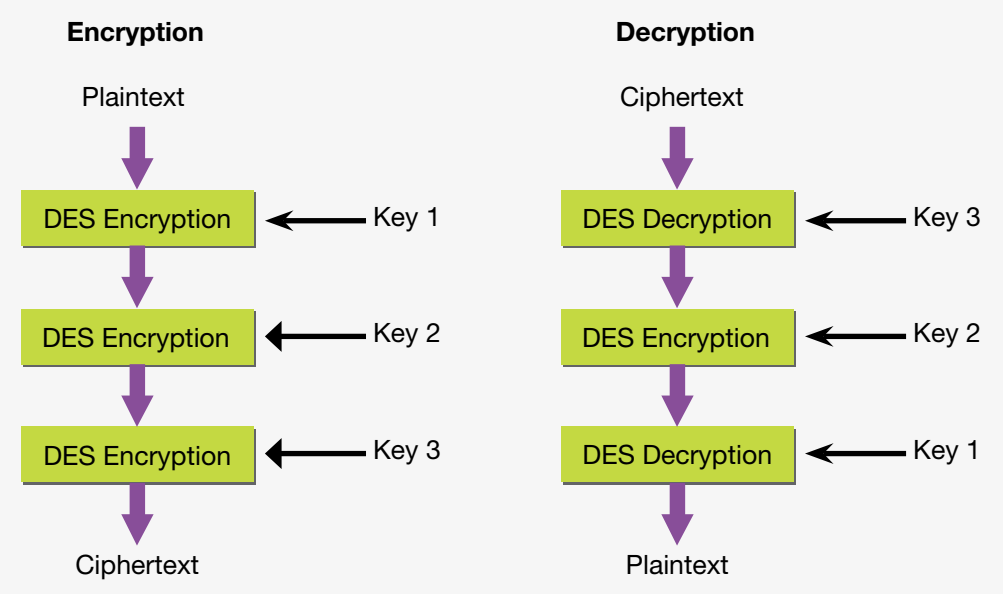


Fig. 6

RSA

RSA is the standard public key encryption algorithm used for encrypting data sent over the internet. It was first described by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology in 1977. Public key cryptography uses **two different but mathematically linked keys** - one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, public and the private keys can encrypt a message, and the other key (from the one used to encrypt a message) is to decode it.

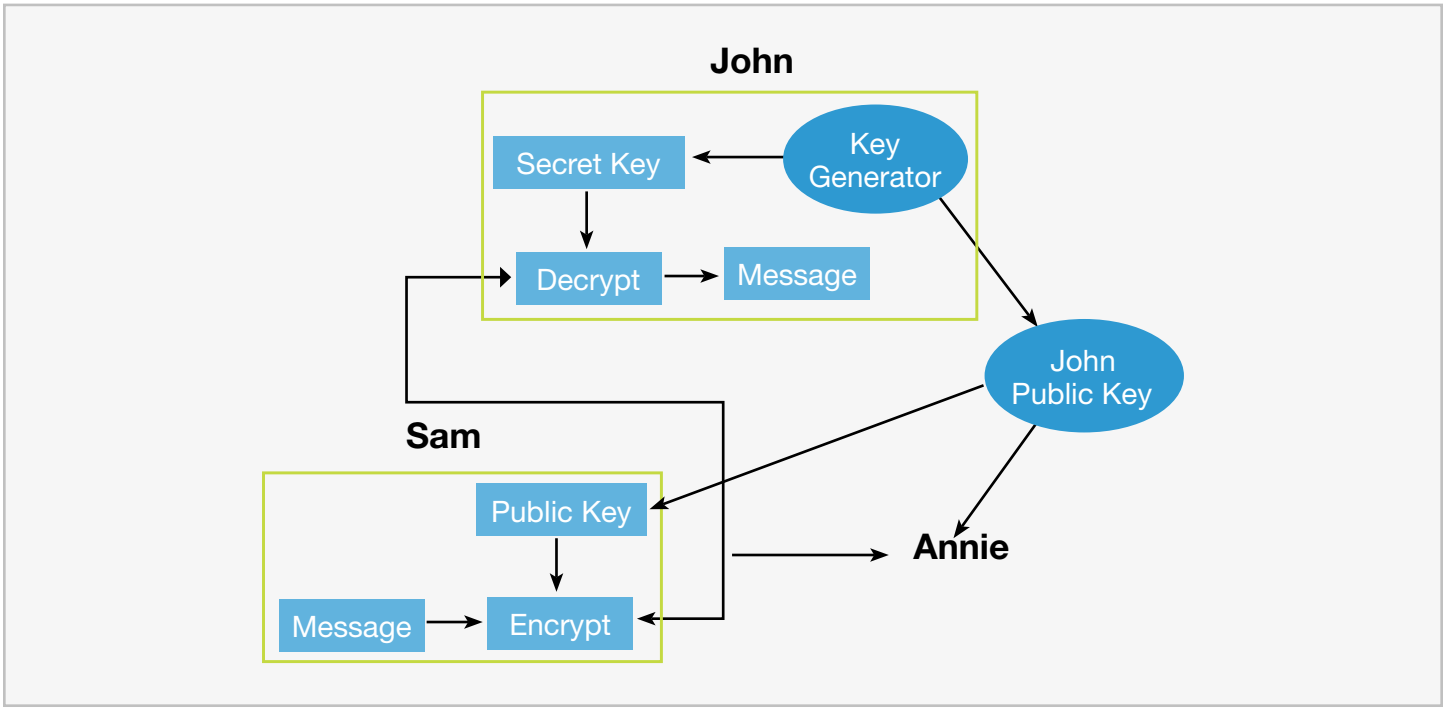


Fig. 7

This feature is one reason why RSA has become the most widely used asymmetric algorithm. It guarantees the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage. The outcome of RSA encryption is a huge batch of shuffled text that takes hackers quite a bit of time and processing power to break.

Blowfish

Blowfish is another algorithm designed to replace DES. It has a 64-bit block size and a **variable key length** ranging from 32-bit up to 448-bit. It comprises of a 16-round Feistel cipher and utilizes huge key-dependent S-boxes.

Every round *r* consists of four actions: First, XOR the left half (L) of the data with the *r*th P-array entry. Second, use the output of XOR function as input for Blowfish's F-function. Next, XOR the F-function's output with the right half (R) of the data, and at last, swap L and R.

The F-function divides the 32-bit input into four 8-bit quarters, and uses the quarters as input to the S-boxes. The S-boxes receives 8-bit input and produce 32-bit output. The outputs are appended with modulo 2^{32} and XORed to produce the final 32-bit output.

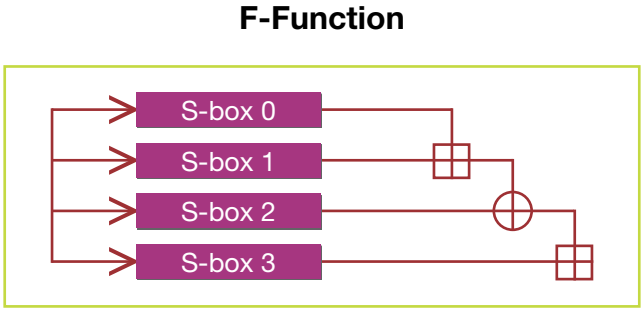


Fig. 8

After the 16th round, undo the last swap and XOR L with P18 and R with P17.

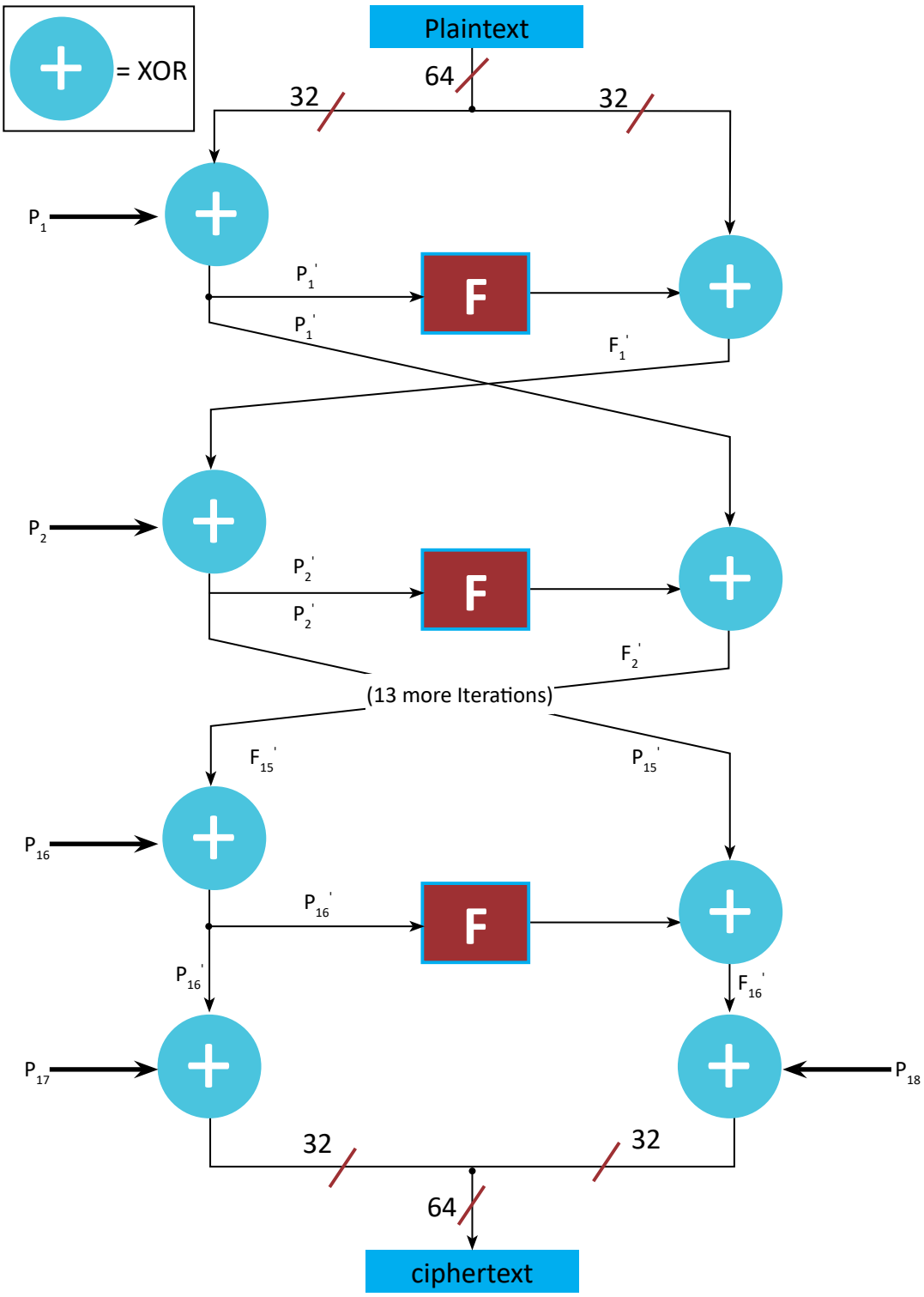


Fig. 9

Blowfish is well-known for its brilliant effectiveness and speed. Vendors have taken full advantage of its free availability within the property right.

Blowfish is getting used in many industries, starting from e-commerce platforms for securing payments to password management tools, wherever it is needed to protect passwords. It's one of the versatile secret writing ways accessible.

Twofish

Blowfish and its successor Twofish, were invented by Bruce Schneier. Keys used in this algorithm can be up to 256-bit in length and as it is a symmetric technique, only one key is needed. The distinctive features of this algorithm is the fact that it uses pre-computed key-dependent S-boxes, and a relatively complex key schedule.

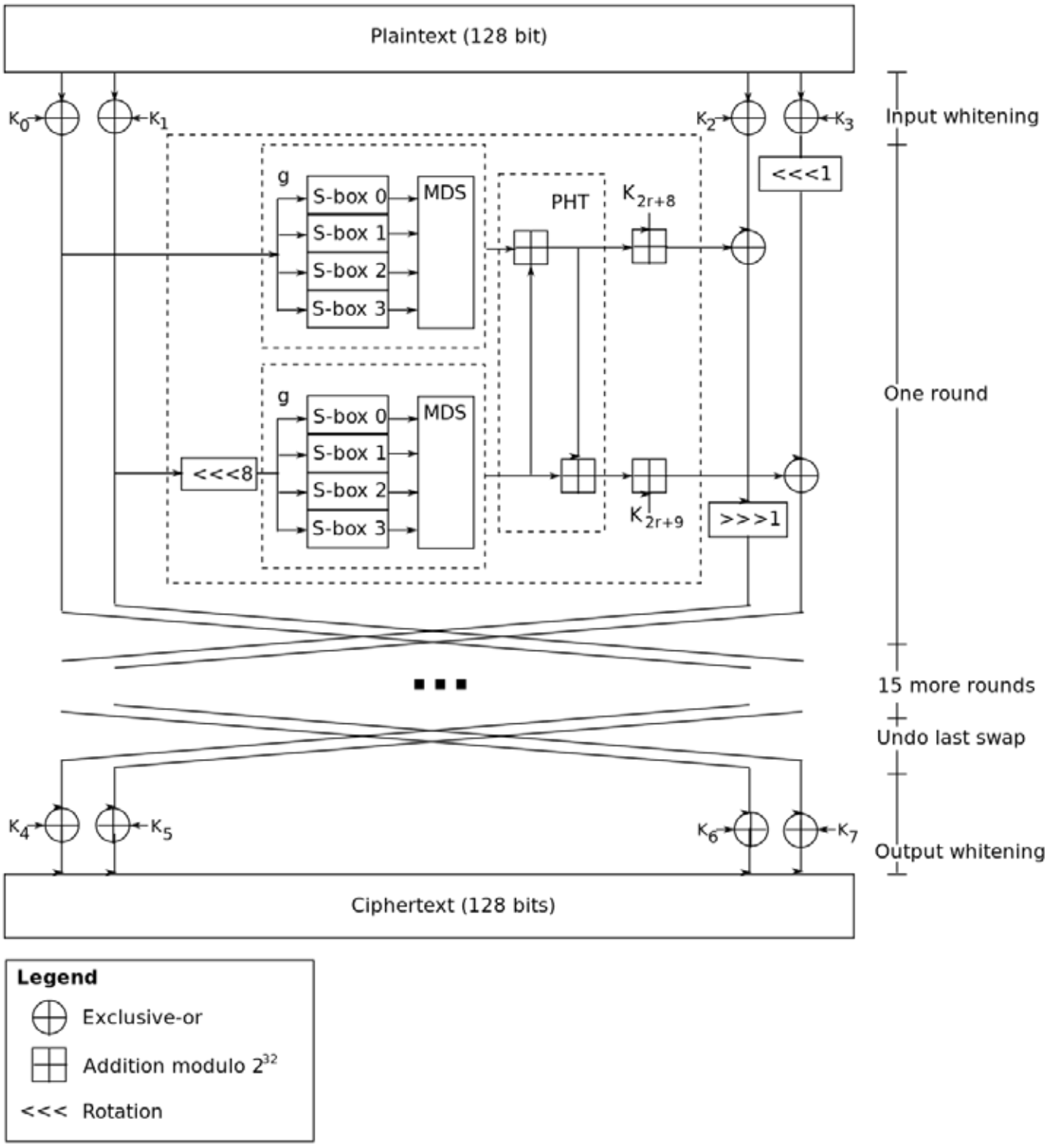


Fig. 10

Twofish is considered as one of the fastest technologies, and an ideal one also to be used in both hardware and software industries. Like Blowfish, Twofish is freely obtainable to anyone. As a result, it is implemented in encryption programs like PhotoEncrypt, GPG, and the popular open source software TrueCrypt.

AES

The Advanced Encryption Standard (AES) is the trusted algorithm by the U.S. Government and numerous organizations.

AES consists of three block ciphers - AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128-bit using keys of 128, 192 and 256-bit, respectively. Although it is extremely effective in 128-bit form, AES also uses keys of 192 and 256-bit for complicated encryption purposes. There are 10 rounds for 128-bit keys; 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys (where a round consists of various processing steps and each round includes substitution, transposition and mixing of the input plaintext, and transformation into the final output of ciphertext).

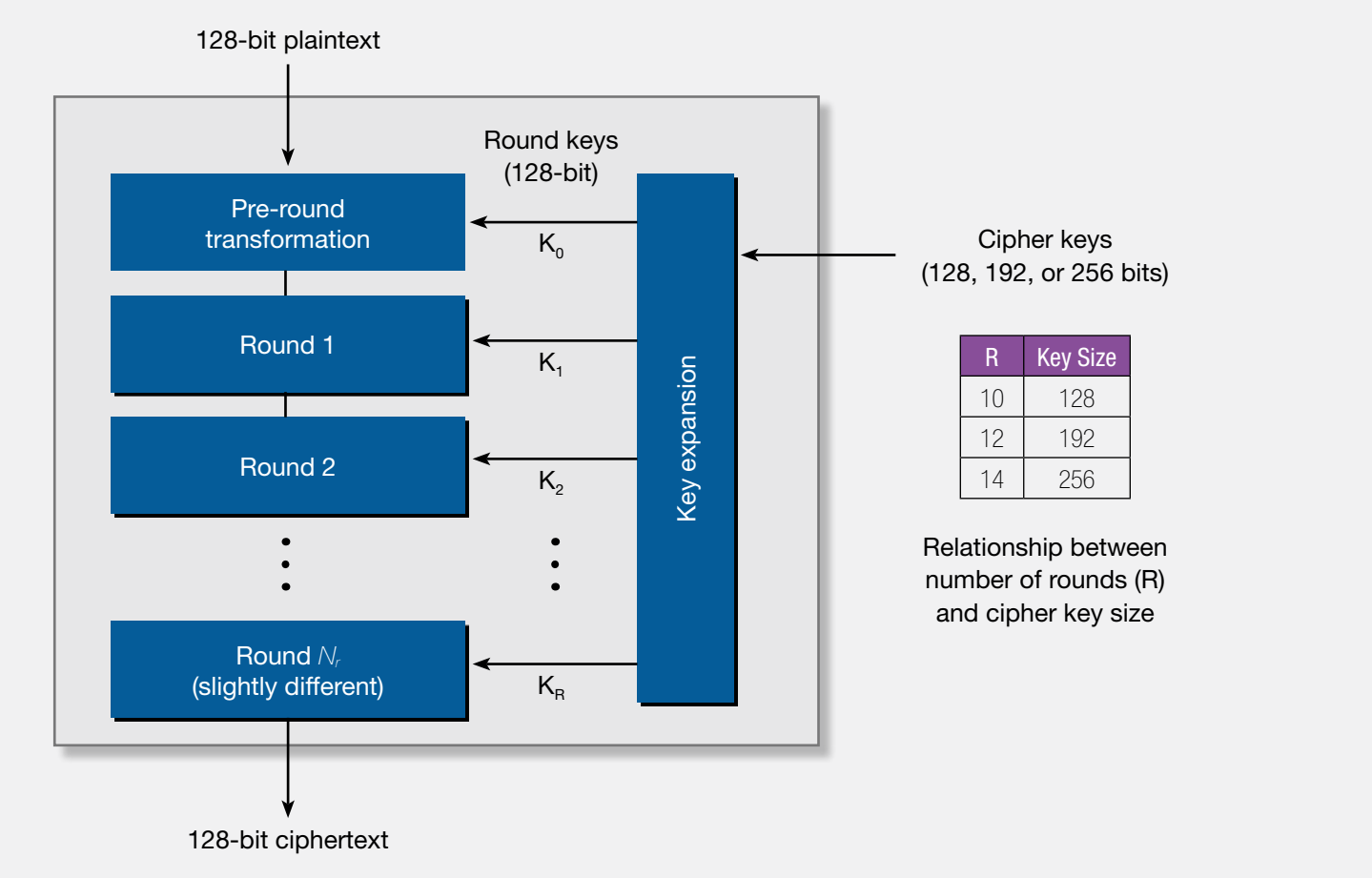


Fig. 11

AES is regarded as oblivious to all attacks, with the exception of the brute force, which tries to decrypt the messages using all possible combinations in the 128, 192, or 256 bits cipher. Still, security experts believe that AES will eventually be hailed as the standardized technique for encrypting data in the private sector.

Benefits and Drawbacks of Cryptography

The network, nowadays, have gone global and information has taken the digital form of bits and bytes. On computer systems and open communication channels critical information is stored, processed and transmitted in digital form. Since information plays an important role, competitors are targeting the systems and communication channels to steal the sensitive information or to interrupt the critical information system.

Modern era cryptography offers a tough set of techniques to make sure that the malevolent intentions of the adversary are prevented while guaranteeing the legitimate users get access to information.

Cryptography – Benefits

Cryptography provides the four most important basic services of information security -

- **Confidentiality** – Encryption technique can prevent the information and communication from unauthorized source and access of information
- **Authentication** – The cryptographic techniques like MAC and digital signatures can protect information against hoax and forgeries
- **Data Integrity** – The cryptographic hash functions play essential role in convincing the users about the data integrity
- **Non-repudiation** – The digital signature imparts the non-repudiation service to secure against the conflict that might occur due to denial of message by the sender

Cryptography – Drawbacks

Although cryptography offers the four basic elements of information security, there are certain issues that affect the effective use of information –

- A heavily encrypted, genuine, and digitally signed **information can be difficult to access** even for a legal user at a crucial time of decision-making. The network or the computer system can be attacked and provide non-functional by an intruder.
- **High availability,** one of the root feature of information security, cannot be ensured through the use of cryptography. Different methods are needed to protect against the threats such as denial of service or complete failure of information system.
- Another basic need of information security of **selective access control** cannot be gained through the use of cryptography. Administrative controls and methods are required to be employed for the same.
- It **does not guard against the vulnerabilities and threats** that arise from the poor design of systems, protocols, and procedures. These need to be rectified through proper design and setting up of a defensive infrastructure.
- More cryptographic techniques in the information processing, more the **delay**
- The use of public key cryptography need setting up and maintenance of public key infrastructure, demanding handsome **financial budget**

Future of Cryptography

There have been recently two potential developments which may have an important influence on cryptography.

- The first is the **development of quantum technology.** In a breakthrough theoretical result in the 1990s, the mathematician Peter Shor revealed the potential of a large scale quantum computer. This utilizes the principles of quantum mechanics to solve the integer factorization and discrete logarithm problems efficiently, thus leaving the RSA and Diffie-Hellman systems insecure.

  While large scale quantum computing technology has not yet been realized (and prospects for its realization remain unclear), the effect that such a realization could have on cryptography cannot be overestimated.

  Fortunately, researchers already have invented two possible approaches to deal with this problem. One is the **development of public key cryptosystems** that are assumed to be safe even against quantum computing attacks. The second approach is **quantum cryptography,** a communication technique that counts on physical assumptions and the laws of quantum physics to provide security.

- The second potential development relates to the **growing usage of cloud computing.** Unfortunately, unless encryption is used to safeguard our stored private data, the privacy of that data from the cloud server (or any other object having access to the cloud server data, such as a hacker) is compromised.

  The use of standard encryption algorithms also has the disadvantage of stopping the server from processing the user data (e.g. to search the data). New types of cryptosystems are currently under progress by the cryptographic research community to overcome this apparent anomaly by allowing the server to process the encrypted data without disclosing the data to the server.

As it can be seen that state-of-the-art in cryptography is presently strong enough to safeguard most of our email and online transactions, but its future status isn't entirely definite. The future, particularly quantum computing, may lead to even more complex cryptographic systems but it can also raise the possibility of new means to break them.

Author

Sruthy Viswanath

Delivery Associate Software Engineer

Sruthy, Delivery Associate Software Engineer, has been with Mphasis for more than a year now. She is a part of Data Engineering Practices, with expertise in Oracle PL/SQL, Mongo DB, SQL Server and SSIS. Sruthy's industry experience includes data migration in Oracle and developing .NET applications

About Mphasis

Mphasis (BSE: 526299; NSE: MPHASIS) applies next-generation technology to help enterprises transform businesses globally. Customer centricity is foundational to Mphasis and is reflected in the Mphasis' Front2Back™ Transformation approach. Front2Back™ uses the exponential power of cloud and cognitive to provide hyper-personalized ($C = X2C^{2}_{TM} = 1$) digital experience to clients and their end customers. Mphasis' Service Transformation approach helps 'shrink the core' through the application of digital technologies across legacy environments within an enterprise, enabling businesses to stay ahead in a changing world. Mphasis' core reference architectures and tools, speed and innovation with domain expertise and specialization are key to building strong relationships with marquee clients. To know more, please visit www.mphasis.com

For more information, contact: nextlabs@mphasis.com

USA
460 Park Avenue South
Suite #1101
New York, NY 10016,
USA
Tel.: +1 212 686 6655

UK
88 Wood Street
London EC2V 7RS, UK
Tel.: +44 20 8528 1000

INDIA
Bagmane World Technology
Center
Marathahalli Ring Road
Doddanakundhi Village,
Mahadevapura
Bangalore 560 048, India
Tel.: +91 80 3352 5000

VAS 18/01/19 US LETTER 4341

www.mphasis.com