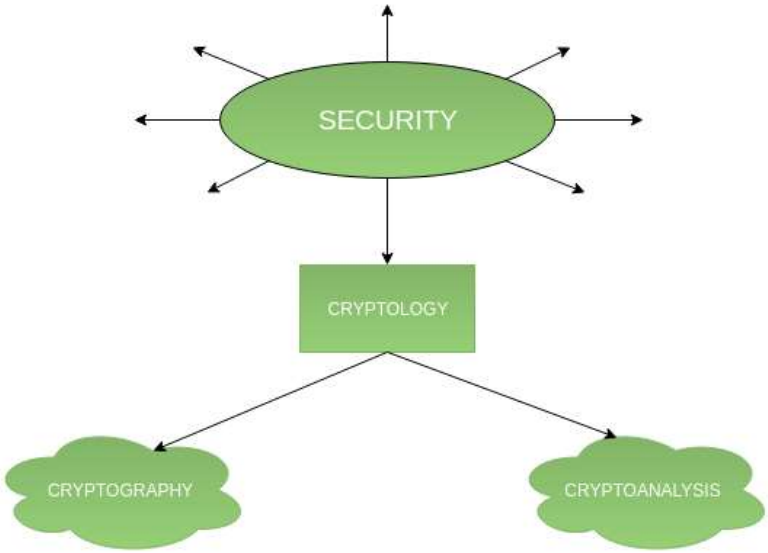
Introduction to Crypto-terminologies

Last Updated : 22 Mar, 2023

Cryptography is an important aspect when we deal with network security. ‘Crypto’ means secret or hidden. Cryptography is the science of secret writing with the intention of keeping the data secret. Cryptanalysis, on the other hand, is the science or sometimes the art of breaking cryptosystems. Both terms are a subset of what is called **Cryptology.**

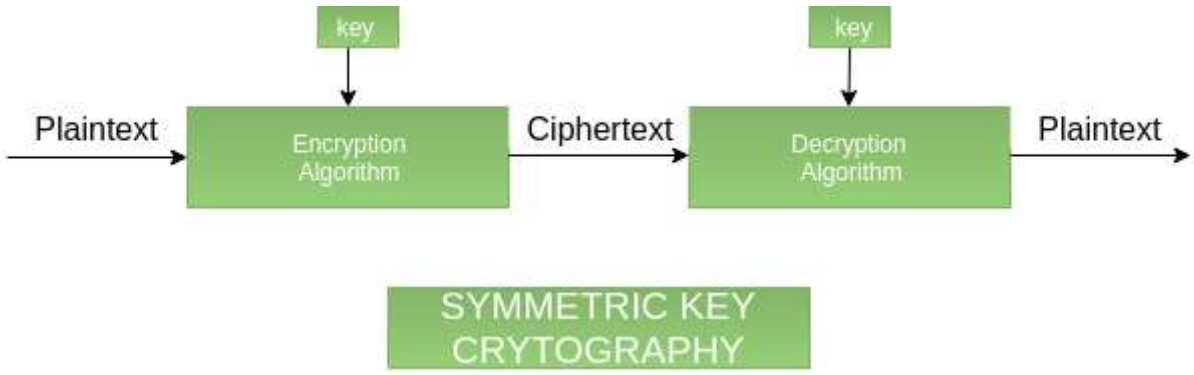
Classification: The flowchart depicts that cryptology is only one of the factors involved in securing networks. Cryptology refers to the study of codes, which involves both writing (cryptography) and solving (cryptanalysis) them. Below is a classification of the crypto terminologies and their various types.



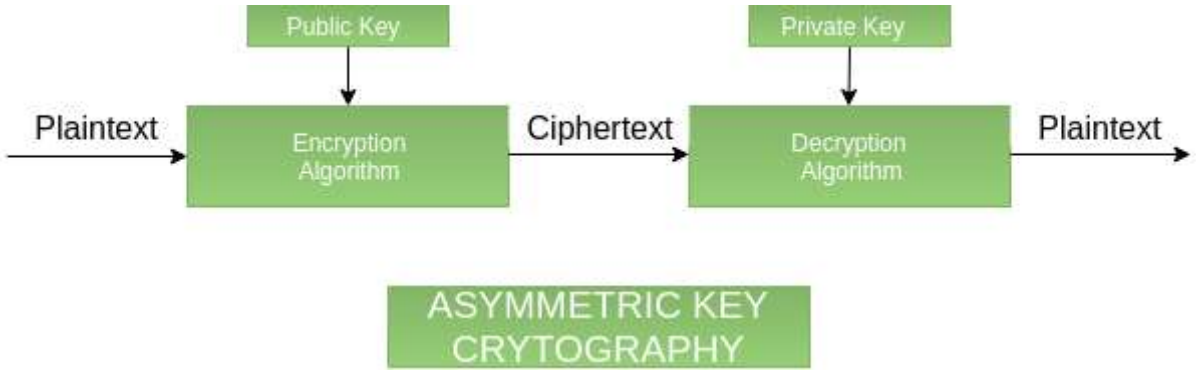
Cryptography:

Cryptography is classified into symmetric cryptography and asymmetric cryptography. Below are the description of these types.

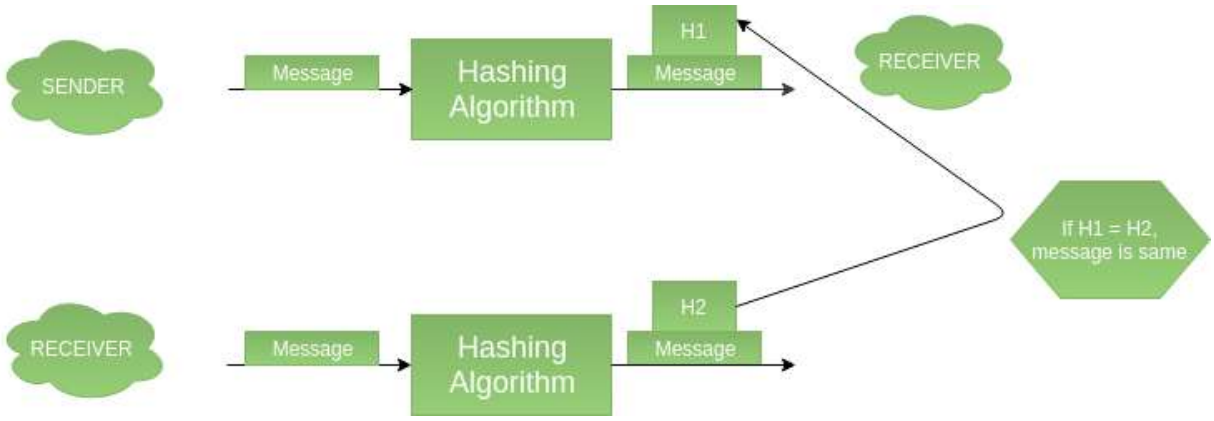
1. **Symmetric key cryptography** – It involves the usage of one secret key along with encryption and decryption algorithms which help in securing the contents of the message. The strength of symmetric key cryptography depends upon the number of key bits. It is relatively faster than asymmetric key cryptography. There arises a key distribution problem as the key has to be transferred from the sender to the receiver through a secure channel.



2. **Asymmetric key cryptography:** It is also known as public-key cryptography because it involves the usage of a public key along with the secret key. It solves the problem of key distribution as both parties use different keys for encryption/decryption. It is not feasible to use for decrypting bulk messages as it is very slow compared to symmetric key cryptography.



3. **Hashing:** It involves taking the plain text and converting it to a hash value of fixed size by a hash function. This process ensures the integrity of the message as the hash value on both, the sender's and receiver's sides should match if the message is unaltered.

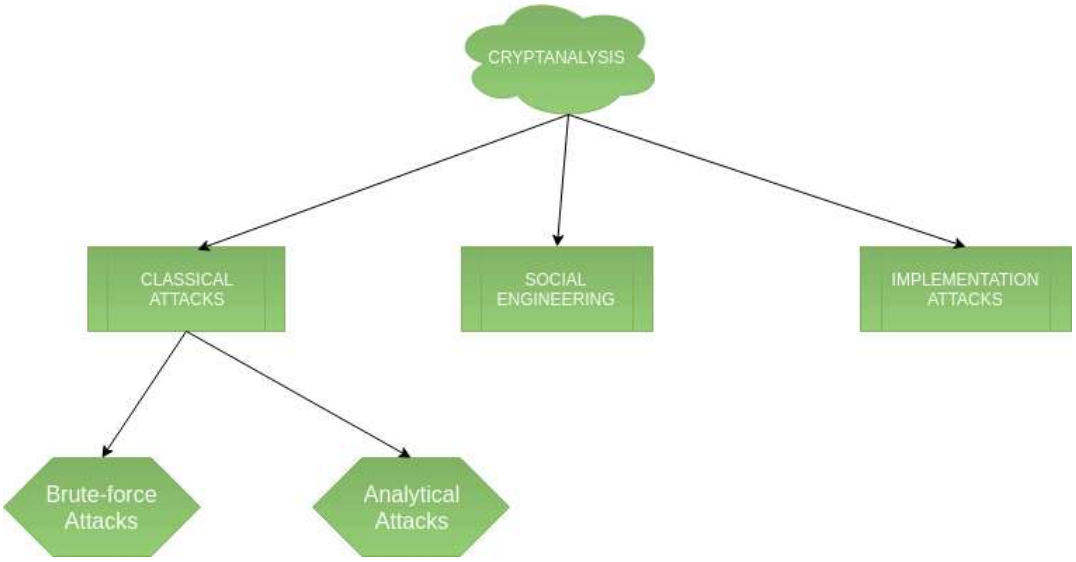


Difference between Hash functions, Symmetric, and Asymmetric algorithms:

Feature	Hash functions	Symmetric algorithms	Asymmetric algorithms
Number of Keys	0	1	2
Length of keys			

Feature	Hash functions	Symmetric algorithms	Asymmetric algorithms
Example	SHA-256, SHA3-256, SHA-512	AES or 3DES	RSA, DSA, ECC

Cryptanalysis:



1. **Classical attacks:** It can be divided into:
   a) Mathematical analysis: It's a type of attack that takes advantage of structural flaws in a specific algorithm.
   b) Brute-force attacks: The attacker uses a Brute Force Attack (BFA) to try all potential keys in order to figure out the key. If the key is long, the attack will take a long time to execute. Brute-force attacks run the encryption algorithm for all possible cases of the keys until a match is found. The encryption algorithm is treated as a black box. Analytical attacks are those attacks that focus on breaking the cryptosystem by analyzing the internal structure of the encryption algorithm.
2. **Social Engineering attack:** It is something that is dependent on the human factor. Tricking someone to reveal their passwords to the attacker or allowing access to the restricted area comes under this attack. People

3. **Implementation attacks:** Implementation attacks such as side-channel analysis can be used to obtain a secret key. They are relevant in cases where the attacker can obtain physical access to the cryptosystem.

Advantages:

1. **Precision:** Crypto-terminologies provide precise and well-defined terms and concepts that help to ensure a clear understanding of the underlying principles of cryptography.
2. **Standardization:** Crypto-terminologies help to standardize the language used in cryptography, which can help to reduce confusion and promote interoperability between different cryptographic systems.
3. **Clarity:** Crypto-terminologies help to promote clarity and accuracy in communication about cryptography, which can help to improve the effectiveness of security measures.
4. **Consistency:** Crypto-terminologies help to ensure consistency in the use of cryptographic concepts and techniques, which can help to reduce the risk of errors or misunderstandings.

Disadvantages:

1. **Complexity:** Crypto-terminologies can be complex and difficult to understand, which can be a barrier to effective communication about cryptography.
2. **Jargon:** Crypto-terminologies can be viewed as jargon by those who are not familiar with the terminology, which can lead to confusion and miscommunication.
3. **Obfuscation:** Crypto-terminologies can be used to obfuscate the true nature of cryptographic techniques, which can be a concern in situations where transparency and openness are important.
4. **Accessibility:** Crypto-terminologies may be inaccessible to those who are not experts in the field, which can limit the ability of non-experts to understand and contribute to discussions about cryptography.

clear." **- Anshika Modi | AIR 21**

37 Suggest improvement

Previous

Difference between Cryptography and Cyber Security

Share your thoughts in the comments Add Your Comment

Similar Reads

Data Communication Terminologies

Terminologies Cache Memory Organization

Crypto Virus

CoinSwitch Becomes first Crypto Platform in India to Reach 2 Crore Users

Introduction of Theory of Computation

Introduction of Mobile Ad hoc Network (MANET)

Introduction of Virtual Router Redundancy Protocol (VRRP) and its configuration

Introduction to TimeStamp and Deadlock Prevention Schemes in DBMS

achivchau...

Article Tags : cryptography , Computer Networks , GATE CS

DevOps Roadmap

Top 15 Websites for CP

System Design

High Level Design
Low Level Design
UML Diagrams
Interview Guide
Design Patterns
OOAD
System Design Bootcamp
Interview Questions

JavaScript

JavaScript Examples
TypeScript
ReactJS
NextJS
AngularJS
NodeJS
Lodash
Web Browser

Preparation Corner

Company-Wise Recruitment Process
Resume Templates
Aptitude Preparation
Puzzles
Company-Wise Preparation

School Subjects

Mathematics
Physics
Chemistry
Biology
Social Science
English Grammar
World GK

Management & Finance

Management
HR Management
Finance
Income Tax
Organisational Behaviour
Marketing

Free Online Tools

Typing Test
Image Editor
Code Formatters
Code Converters
Currency Converter
Random Number Generator
Random Password Generator

More Tutorials

Software Development
Software Testing
Product Management
SAP
SEO - Search Engine Optimization
Linux
Excel

GeeksforGeeks Videos

DSA
Python
Java
C++
Data Science
CS Subjects