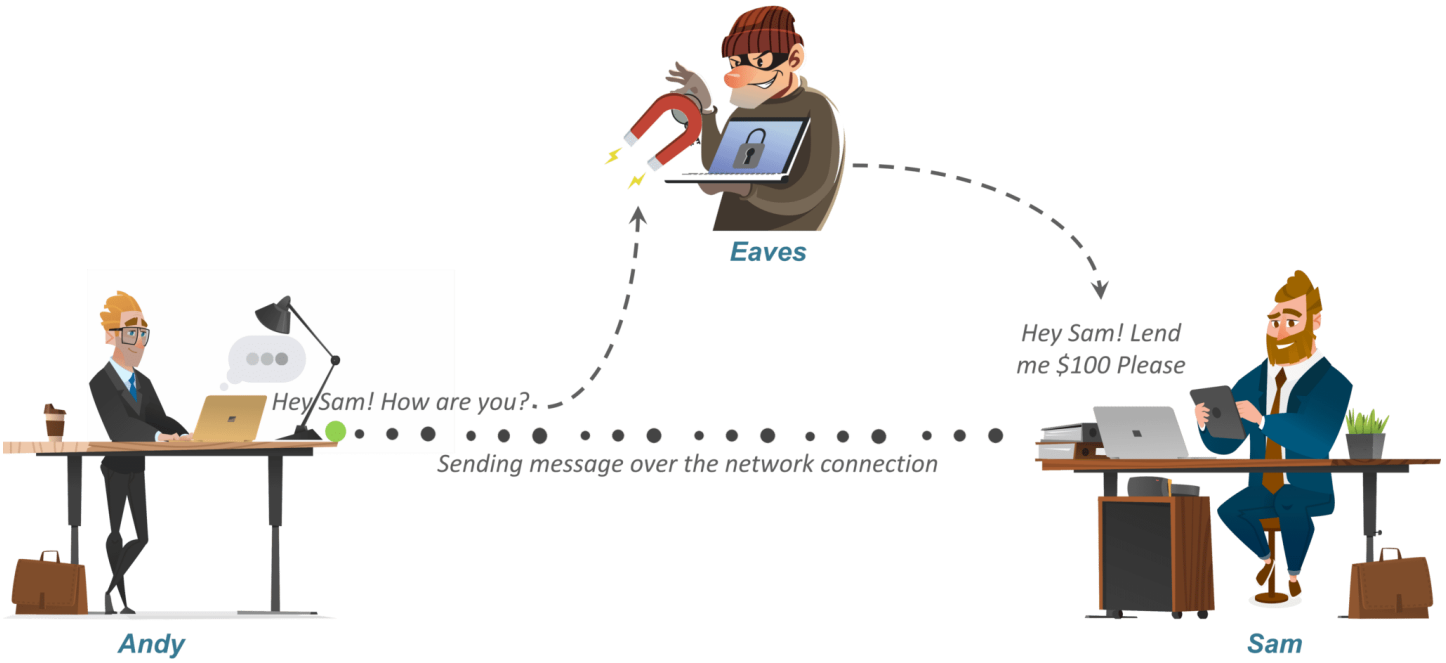
CRYPTUS CYBER
SECURITY PVT. LTD.

# Module Name:

## Cryptography Analysis



## INTRODUCTION TO CRYPTOGRAPHY

*Cryptography is a form of Encryption itself, where a readable plain text format is converted into another form which doesn't leave the value of the plain text as it was before but the basic difference will be, the converted form will be readable by the human beings but will be of no sense. These encryption technique is used mostly for securing and maintaining the privacy of the data.*

*For this technique user had to have a Encryption Algorithm and a Key for its Decryption. User will transmit that encrypted message, Receiver will receive. Now for the receiver to understand, he needs to convert it into plain text, cipher, for that he again needs the key and the exact algorithm (decryption).*

### *TERMINOLOGIES:*

*Plain Text: A text which is created and readable by the individuals only.*
*Cipher Text: It is the encrypted text, which is converted by applying an algorithm on the plain text.*
*Encryption: Process of converting a plain text to cipher text.*
*Decryption: Process of converting a cipher text to plain text.*

### *CIPHERS:*

*In Cryptography process, Ciphers are those encrypted text which came through the algorithm process of encryption.*

### *Example of Cipher:*

*Caesar Cipher is one of the oldest ciphers which came across with the technique of encrypting a plain text into a Cipher Text. Caesar Cipher works by adding or subtracting 3 characters of that particular number. That means if in a Plain Text there is a Character E either it will be transferred it to B and if the character is A it will be transferred to X.*

*This Cipher algorithm is having some mathematical equations which describe the functionality of a cryptography process.*

*Further examples of these Ciphers are Hill Climb and Play Fair Cipher.*

### *KEY SYSTEM IN CRYPTOGRAPHY:*

*A cryptographic key is that bits used of data which are use by cryptographic algorithms for converting plain text into cipher text or vice versa.*
*There are mainly two Cryptographic Keys.*

*ASYMMETRIC KEY / PUBLIC KEY CRYPTOGRAPHY: Asymmetric key encryption algorithms called public key algorithms use two different but related keys for encryption and decryption and is publicly provided by the Web Server.*
*SYMMETRIC KEY / PRIVATE KEY CRYPTOGRAPHY: Symmetric key encryption algorithms use a single symmetric key for both encryption and decryption and is a privately kept.*

## *STEGANOGRAPHY:*

*Steganography is a process in which we basically hide a data inside a data.*
*This is the process in which the data is hidden into the Plain Sight or a Image, Audio or a Video file. This process can also be used along with cryptography as an extra-secure method in which to protect data.*
*One of the most famous and simplest technique used in Steganography is least significant bit technique also known as LSB.*

## *STEPS:*

*$ CMD > copy /b Jelly.jpg+list.txt steganography.jpg*

*Here, /b is used for Binding the 2 files, Copy is used for copying the content of second file to first file.*

*For using Cryptography with Steganography, we can use "Encipher.it".*
*prabhankar > +1 > qsbcibolbs >*

## *Hashes:*

*It converts data into either alpha numeric form or in hex form. But there is a difference between a cipher encryption and a hash. The difference is encrypted text can be reverted and further decrypted, but hashes cannot be reverted. We need to crack the hashes.*
*Hash function is that which takes an input and returns a fixed-size alphanumeric string. The string is called the hash value. Examples MD5 Hash, Base64 Encoding etc.*

*EG. alphanumeric - scusege67dg367df7fd3fd37f3636d*

## *MD5 Examples:*

*a > 0cc175b9c0f1b6a831c399e269772661*
*aaaa> 594f803b380a41396ed63dca39503542*
*28ecc377359fc5df5a4a8ed174ecc151:*
*Hello Sidharth sir, I hope your phone is fine, and I forgot to tell you, during the session, i got your backups of whatsapp chats.*

*BASE 64 EXAMPLES:*

*ALTAMASH > QUxUQU1BU0gK*
*SANJEEV > U0FOSkVFVgo*
*Hello Sidharth sir, I hope your phone is fine, and I forgot to tell you, during the session, i got your backups of whatsapp chats>*
*SGVsbG8gU2lkaGFydGggc2lyLCBJIGhvcGUgeW91ciBwaG9uZSBpcyBmaW5lLCBhbmQgSSBmb3Jnb3QgdG8gdGVsbCB5b3UsIGR1cmluZyB0aGUgc2Vzc2lvbiwgaSBnb3QgeW91ciBiYWNrdXBzIG9mIHdoYXRzYXBwIGNoYXRzLiA=*

*Cracking methods for Hashes : We have to create a dictionary and have to convert every word into the hash of a particular wordlists, and after that we will compare that particular hash. If matches it means that the specific word is found. Hashes are usually uniques.*
*HASHES FORMATS:*

*1. Base64 encoding*
*It is the process of encoding, in which the plain text is converted into the alpha numeric form, but the length of the hash varies as per the length of the plain text. It's a textual encoding of binary data where the resultant text has nothing but letters, numbers and the symbols.*

*Examples:*

*password - cGFzc3dvcmQ, admin - YWRtaW4 , administrator - YWRtaW5pc3RyYXRvcg*

*2. MD5 (Message Digest 512 bit)*
*It will convert the plain text into hexadecimal text of fixed length. It always creates a unique hash for the plain text and are normally shown in their 32 digit hexadecimal value equivalent.*
*Examples:*
*password - 5f4dcc3b5aa765d61d8327deb882cf99*
*admin - 21232f297a57a5a743894a0e4a801fc3*
*administrator - 200ceb26807d6bf99fd6f4f0d1ca54da4*

*3. SHA 256/512*

*AUTOMATED TOOL:*

*Hashcat is the world's fastest and most advanced password recovery tool. It is the fastest hash recovery tool which converts the wordlist into the hashes and then matches those hashes with the specific hash we want to recover. It is pre-installed in kali linux OS.*

*Instead of using standard CPU cores, it will use GPU or Graphic card cores.*

*USAGE :*

*$ hashcat -m 0 -a 3 <hashfile in txt> <dictionary/wordlist>*

*STEPS :*

*$ hashcat -m 0 -a 3 /root/Desktop/hash.txt /usr/share/wordlists/rockyou.txt*

*$ hashcat -m 0 -a 3 /root/Desktop/hash.txt /usr/share/wordlists/rockyou.txt --force*

*Here,*
*hashcat is the tool for password recovery*
*- m: hash type*
*0: MD5*
*-a: attack mode*
*3: Brute force attack*
*hash.txt: file containing hashes to be recovered*
*rockyou.txt: for brute forcing and comparing*
*--force: to start forcefully*

*CUDA CRACKING*

*CUDA Cracking also called GPU Password Cracking is only for NVidia. Cuda is the part of NVidia only, so Graphic cards which are of NVidia can support cuda cracking, which makes the password recovery very fast.*

## Cryptanalysis:

*Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them. For example, cryptanalysts seek to decrypt ciphertexts without knowledge of the plaintext source, encryption key or the algorithm used to encrypt it; cryptanalysts also target secure hashing, digital signatures and other cryptographic algorithms.*

*While the objective of cryptanalysis is to find weaknesses in or otherwise defeat cryptographic algorithms, cryptanalysts' research results are used by cryptographers to improve and strengthen or replace flawed algorithms. Both cryptanalysis, which focuses on deciphering encrypted data, and cryptography, which focuses on creating and improving encryption ciphers and other algorithms, are aspects of cryptology, the mathematical study of codes, ciphers and related algorithms.*

*Researchers may discover methods of attack that completely break an encryption algorithm, which means that ciphertext encrypted with that algorithm can be decrypted trivially without access to the encryption key. More often, cryptanalytic results uncover weaknesses in the design or implementation of the algorithm, which can reduce the number of keys that need to be tried on the target ciphertext.*

*For example, a cipher with a 128 bit encryption key can have $2^{128}$ (or 340,282,366,920,938,463,463,374,607,431,768,211,456) unique keys; on average, a brute force attack against that cipher will succeed only after trying half of those unique keys. If cryptanalysis of the cipher reveals an attack that can reduce the number of trials needed to $2^{40}$ (or just 1,099,511,627,776) different keys, then the algorithm has been weakened significantly, to the point that a brute-force attack would be practical with commercial off-the-shelf systems.*

*Cryptanalysis is practiced by a broad range of organizations, including governments aiming to decipher other nations' confidential communications; companies developing security products that employ cryptanalysts to test their security features; and hackers, crackers, independent researchers and academicians who search for weaknesses in cryptographic protocols and algorithms. It is this constant battle between cryptographers trying to secure information and cryptanalysts trying to break cryptosystems that moves the entire body of cryptology knowledge forward.*

## *Cryptanalysis techniques and attacks*

*There are many different types of cryptanalysis attacks and techniques, which vary depending on how much information the analyst has about the ciphertext being analyzed. Some cryptanalytic methods include:*

- *In a ciphertext-only attack, the attacker only has access to one or more encrypted messages but knows nothing about the plaintext data, the encryption algorithm being used or any data about the cryptographic key being used. This is the type of challenge that intelligence agencies often face when they have intercepted encrypted communications from an opponent.*
- *In a known plaintext attack, the analyst may have access to some or all of the plaintext of the ciphertext; the analyst's goal in this case is to discover the key used to encrypt the message and decrypt the message. Once the key is discovered, an attacker can decrypt all messages that had been encrypted using that key. Linear cryptanalysis is a type of known plaintext attack that uses a linear approximation to describe how a block cipher Known plaintext attacks depend on the attacker being able to discover or guess some or all of an encrypted message, or even the format of the original plaintext. For example, if the attacker is aware that a particular message is addressed to or about a particular person, that person's name may be a suitable known plaintext.*
- *In a chosen plaintext attack, the analyst either knows the encryption algorithm or has access to the device used to do the encryption. The analyst can encrypt the chosen plaintext with the targeted algorithm to derive information about the key.*
- *A differential cryptanalysis attack is a type of chosen plaintext attack on block ciphers that analyzes pairs of plaintexts rather than single plaintexts, so the analyst can determine how the targeted algorithm works when it encounters different types of data.*
- *Integral cryptanalysis attacks are similar to differential cryptanalysis attacks, but instead of pairs of plaintexts, it uses sets of plaintexts in which part of the plaintext is kept constant but the rest of the plaintext is modified. This attack can be especially useful when applied to block ciphers that are based on substitution-permutation networks.*
- *A side-channel attack depends on information collected from the physical system being used to encrypt or decrypt. Successful side-channel attacks use data that is neither the ciphertext resulting from the encryption process nor the plaintext to be encrypted, but rather may be related to the amount of time it takes for a system to respond to specific queries, the amount of power consumed by the*

*encrypting system, or electromagnetic radiation emitted by the encrypting system.*

- *A dictionary attack is a technique typically used against password files and exploits the human tendency to use passwords based on natural words or easily guessed sequences of letters or numbers. The dictionary attack works by encrypting all the words in a dictionary and then checking whether the resulting hash matches an encrypted password stored in the SAM file format or other password file.*
- *Man-in-the-middle attacks occur when cryptanalysts find ways to insert themselves into the communication channel between two parties who wish to exchange their keys for secure communication via asymmetric or public key infrastructure The attacker then performs a key exchange with each party, with the original parties believing they are exchanging keys with each other. The two parties then end up using keys that are known to the attacker.*

*Other types of cryptanalytic attacks can include techniques for convincing individuals to reveal their passwords or encryption keys, developing Trojan horse programs that steal secret keys from victims' computers and send them back to the cryptanalyst, or tricking a victim into using a weakened cryptosystem. Side-channel attacks have also been known as timing or differential power analysis. These attacks came to wide notice in the late 1990s when cryptographer Paul Kocher was publishing results of his research into timing attacks and differential power analysis attacks on Diffie-Hellman, RSA, Digital Signature Standard (DSS) and other cryptosystems, especially against implementations on smart cards.*

## *Tools for cryptanalysis*

*Because cryptanalysis is primarily a mathematical subject, the tools for doing cryptanalysis are in many cases described in academic research papers. However, there are many tools and other resources available for those interested in learning more about doing cryptanalysis. Some of them include:*

- *CrypTool is an open source project that produces e-learning programs and a web portal for learning about cryptanalysis and cryptographic algorithms.*

- *Cryptol is a domain-specific language originally designed to be used by the National Security Agency specifying cryptographic algorithms. Cryptol is published under an open source license and available for public use. Cryptol makes it possible for users to monitor how algorithms operate in software programs written to specify the algorithms or ciphers. Cryptol can be used to deal with cryptographic routines rather than with entire cryptographic suites.*
- *CryptoBench is a program that can be used to do cryptanalysis of ciphertext generated with many common algorithms. It can encrypt or decrypt with 29 different symmetric encryption algorithms; encrypt, decrypt, sign and verify with six different public key algorithms; and generate 14 different kinds of cryptrographic hashes as well as two different types of checksum.*
- *Ganzúa (meaning picklock or skeleton key in Spanish) is an open source cryptanalysis tool used for classical polyalphabetic and monoalphabetic ciphers. Ganzúa lets users define nearly completely arbitrary cipher and plain alphabets, allowing for the proper cryptanalysis of cryptograms obtained from non-English text. A Java application, Ganzúa can run on Windows, Mac OS X or Linux.*

*Cryptanalysts commonly use many other data security tools including network sniffers and password cracking software, though it is not unusual for cryptanalytic researchers to create their own custom tools for specific tasks and challenges.*

## *Requirements and responsibilities for cryptanalysts*

*A cryptanalyst's duties may include developing algorithms, ciphers and security systems to encrypt sensitive information and data and analyzing and decrypting different types of hidden information, including encrypted data, cipher texts and telecommunications protocols, in cryptographic security systems.*

*Government agencies as well as private sector companies hire cryptanalysts to ensure their networks are secure and sensitive data transmitted through their computer networks is encrypted.*

*Other duties that cryptanalysts may be responsible for include:*

- *Protecting critical information from being intercepted copied, modified or deleted.*
- *Evaluating, analyzing and targeting weaknesses in cryptographic security systems and algorithms.*
- *Designing security systems to prevent vulnerabilities.*
- *Developing mathematical and statistical models to analyze data and solve security problems.*
- *Testing computational models for accuracy and reliability.*
- *Investigating, researching and testing new cryptology theories and applications.*
- *Searching for weaknesses in communication lines.*
- *Ensuring financial data is encrypted and accessible only to authorized users.*
- *Ensuring message transmission data isn't hacked or altered in transit.*
- *Decoding cryptic messages and coding systems for military, law enforcement and other government agencies.*
- *Developing new methods to encrypt data as well as new methods to encode messages to conceal sensitive data.*

*Individuals planning to pursue a career in cryptanalysis are advised to obtain a bachelor's degree in computer science, computer engineering, mathematics or a related field; some organizations will consider hiring individuals without a technical degree if they have extensive training and prior work experience in the field.*

*A Master of Science degree is also strongly recommended, unless the candidate already has a bachelor's degree in mathematics and computer science. The strongest candidates will have a doctoral degree in mathematics or computer science with a focus on cryptography.*