Cryptanalysis and Brute-Force Attack

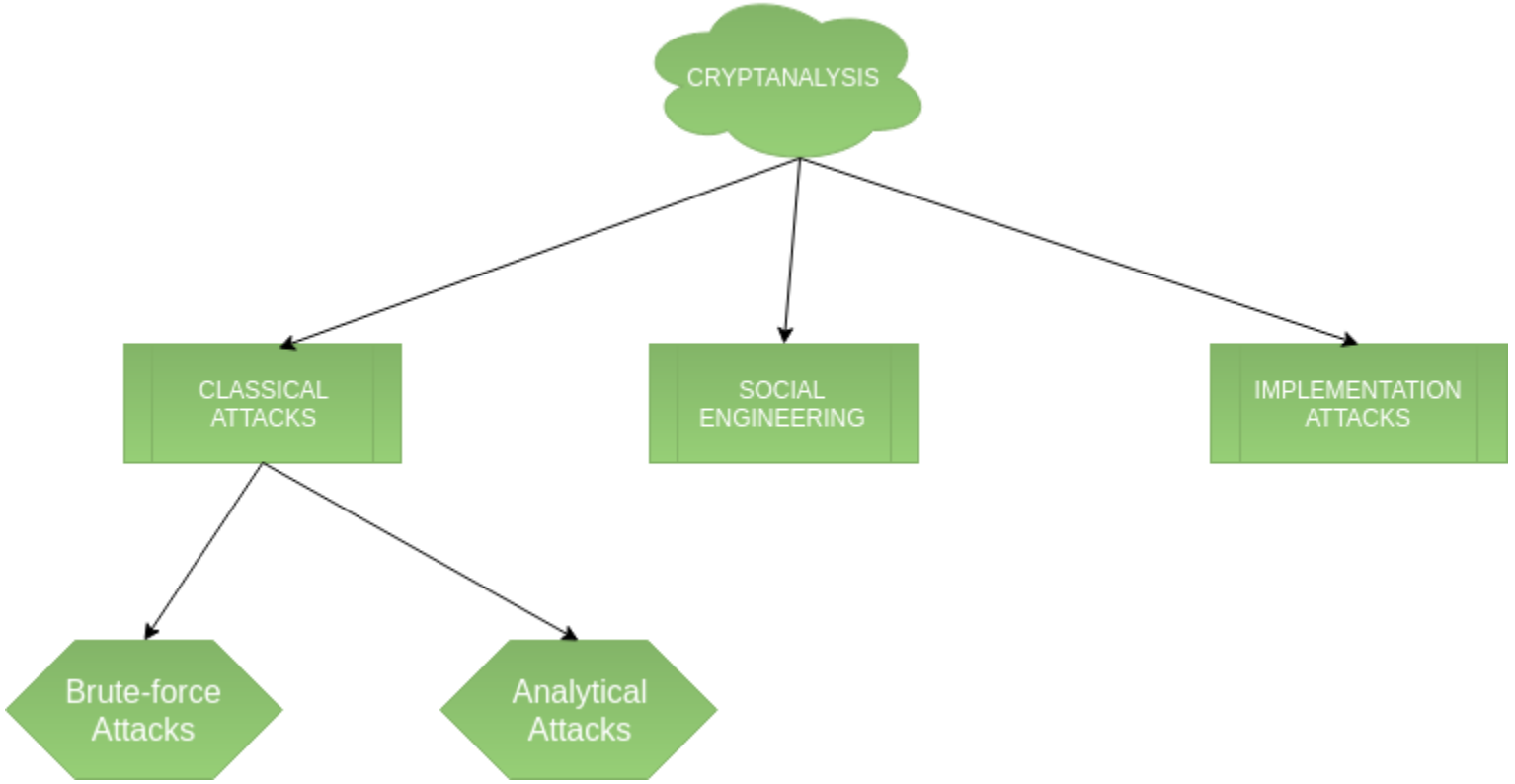
B Tech CSE- IV Sem

TCS 491

Introduction to Cryptography

Jan- Jun 2022

Cryptanalysis –



Cryptanalysis and Brute-Force Attack

- Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:
- ■ Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- ■ Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

1. **Classical attacks –**
   It can be divided into a)Mathematical analysis and b) Brute-force attacks. Brute-force attacks runs the encryption algorithm for all possible cases of the keys until a match is found. Encryption algorithm is treated as a black box. Analytical attacks are those attacks which focuses on breaking the cryptosystem by analysing the internal structure of the encryption algorithm.
2. **Social Engineering attack –**
   It is something which 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 should be cautious when revealing their passwords to any third party which is not trusted.
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.

- Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

- Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Given table summarizes the various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst

Type of Attack	Known to Cryptanalyst
Ciphertext Only	■ Encryption algorithm ■ Ciphertext
Known Plaintext	■ Encryption algorithm ■ Ciphertext ■ One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	■ Encryption algorithm ■ Ciphertext ■ Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	■ Encryption algorithm ■ Ciphertext ■ Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	■ Encryption algorithm ■ Ciphertext ■ Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key ■ Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Brute Force Attack

- A **Brute force attack** is a well known breaking technique, by certain records, brute force attacks represented five percent of affirmed security ruptures. A brute force attack includes ‘speculating’ username and passwords to increase unapproved access to a framework. Brute force is a straightforward attack strategy and has a high achievement rate.
- A few attackers use applications and contents as brute force devices. These instruments evaluate various secret word mixes to sidestep confirmation forms. In different cases, attackers attempt to get to web applications via scanning for the correct session ID. Attacker inspiration may incorporate taking data, contaminating destinations with malware, or disturbing help.
- While a few attackers still perform brute force attacks physically, today practically all brute force attacks are performed by bots. Attackers have arrangements of usually utilized accreditations, or genuine client qualifications, got through security breaks or the dull web. Bots deliberately attack sites and attempt these arrangements of accreditations, and advise the attacker when they obtain entrance.

BRUTE-FORCE ATTACK

- A brute-force attack involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success.
- That is, if there are X different keys, on average an attacker would discover the actual key after X/2 tries.
- It is important to note that there is more to a brute-force attack than simply running through all possible keys.
- Unless known plaintext is provided, the analyst must be able to recognize plaintext as plaintext. If the message is just plain text in English, then the result pops out easily, although the task of recognizing English would have to be automated.
- If the text message has been compressed before encryption, then recognition is more difficult. And if the message is some more general type of data, such as a numerical file, and this has been compressed, the problem becomes even more difficult to automate.
- Thus, to supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed.

Types of Brute Force Attacks:

1. **Simple brute force attack:** utilizes an efficient way to deal with ‘surmise’ that doesn’t depend on outside rationale.
2. **Dictionary attacks –** surmises usernames or passwords utilizing a dictionary of potential strings or phrases
3. **Hybrid brute force attacks** begins from outer rationale to figure out which password variety might be destined to succeed, and afterward proceeds with the simple way to deal with attempt numerous potential varieties.
4. **Reverse brute force attack –** utilizes a typical password or assortment of passwords against numerous conceivable usernames. Focuses on a network of clients for which the attackers have recently acquired information.
5. **Credential stuffing –** utilizes beforehand known password-username sets, attempting them against numerous sites. Adventures the way that numerous clients have the equivalent username and password across various frameworks.

Cryptographic systems are characterized along three independent dimensions:

- 1. The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (i.e., that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.
- 2. The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.
- 3. The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Thank You

&

Best Wishes