15.4.2 Cryptanalysis and Cryptographic Attack Countermeasures Facts

Cryptanalysis is the study of ciphers, ciphertext, or cryptosystems with the intent to identify vulnerabilities that allow plain text to be extracted from the ciphertext, even if the cryptographic key or algorithm used to encrypt the plain text is unknown.

This lesson covers the following topics:

- Types of cryptanalysis
- Code breaking methods
- Cryptography attacks
- Cryptographic attack countermeasures

Types of Cryptanalysis

There are three types of cryptanalysis methods.

- Linear cryptanalysis is based on finding the linear, or affine, approximation to the action of a cipher. It is commonly used on block ciphers and works on statistical differences between plain text and ciphertext.
- Differential cryptanalysis is a form of cryptanalysis applicable to symmetric key algorithms and works on statistical differences between ciphertexts of chosen data.
- Integral cryptanalysis is useful against block ciphers based on substitution-permutation networks. It is an extension of differential cryptanalysis.

Code Breaking Methods

There are several code breaking methods.

- Brute force is one of the most commonly used methods. In a brute force attack, the cryptography keys are discovered by trying every possible combination.
- Frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext. It works on the assumption that in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies.
- Trickery and deceit is using social engineering techniques to extract cryptography keys.
- The one-time pad method uses many non-repeating groups of letters or number keys that are chosen randomly.

Cryptography Attacks

A hacker will try to obtain any information that has enough perceived value. Cryptographic attacks can use many methods to attempt to bypass the encryption someone is using. The hacker might focus on a code weakness, the cipher, the protocol, or even key management. Even if a hacker cannot decrypt the data, there may be valuable information from monitoring the flow of traffic. To avoid this problem, some organizations set up systems to maintain a steady flow of encrypted traffic.

The following table describes several cryptography attacks.

Attack	Description
Ciphertext-only	The goal of this attack type is to recover the encryption key from the ciphertext. This attack requires a hacker to obtain encrypted messages that have been encrypted using the same encryption algorithm. Ciphertext attacks don't require the hacker to have the plain text; the statistical analysis might be enough.
Adaptive chosen plain text	In a adaptive chosen plain text method, the hacker makes a series of interactive queries, choosing subsequent plain texts based on the information from the previous encryptions.
Chosen plain text	In a chosen plain text attack, the hacker creates plain text, feeds it into the cipher, and analyzes the resulting ciphertext. The chosen plain text attack occurs when the hacker can choose the information to be encrypted. The idea is to find patterns in the cryptographic output that might uncover a vulnerability or reveal the cryptographic key.
Related key	In a related key attack, the hacker obtains ciphertexts encrypted under two different keys. This attack is useful if the hacker can obtain the plain text and matching ciphertext.
Dictionary	In a dictionary attack, the attacker constructs a dictionary of plain text along with its corresponding ciphertext collected over a period of time.
Known plain text	In this attack, the only information available to the attacker is some plain text blocks, the corresponding ciphertext, and the algorithm used to encrypt and decrypt the text. This attack requires the hacker to have both the plain text and ciphertext of one or more messages. Together, these two items can be used to extract the cryptographic key and decrypt the remaining encrypted files.
Chosen ciphertext	In a chosen ciphertext attack, the hacker analyzes the plain texts corresponding to an arbitrary set of ciphertexts the hacker chooses. Early versions of RSA used in SSL were vulnerable to this attack.

Rubber hose	In a rubber hose attack, a hacker extracts cryptographic secrets, such as the password to an encrypted file, by coercion or torture.
Chosen key	A chosen key attack is a type of attack where a hacker not only breaks a ciphertext, but also breaks into a bigger system, which is dependent on that ciphertext.
Timing	The timing attack is based on repeatedly measuring the exact execution times of modular exponentiation operations.

Some of the tools used to break ciphers are the CrypTool project, which develops e-learning programs in the area of cryptography and cryptanalysis. It consists of e-learning software CT1, CT2, JCT, and CTO. MD5 Decryption Tool and MD5 Decoder are also tools used to break ciphers.

Cryptographic Attack Countermeasures

The countermeasures used to keep hackers from using various cryptanalysis methods and techniques are:

- Restrict access to cryptographic keys. Keys should be given to the application or to the user directly.
- An intrusion detection system should be deployed to monitor the exchange and access of keys.
- Passphrases and passwords should be used to encrypt the key if it is stored on disk.
- Keys should not be present inside the source code or binaries.
- For certificate signing, transfer of private keys should be prohibited.
- For symmetric algorithms, use a key size of 168 bits or 256 bits, especially in case of large transactions.