9.4.2 Cryptographic Attack Facts

Cryptanalysis is the method of recovering original data that has been encrypted without having access to the key used in the encryption process. This can be done to measure and validate the strength of a cryptosystem. It can also be done to violate the confidentiality and/or integrity of a cryptosystem.

The security of data depends on the secrecy of the keys, not on the algorithm used to encrypt the data. For this reason, the less information the attacker has concerning the key used during encryption, the stronger the security. Most cryptographic attacks focus on breaking the key. Attacks can be classified using one of the following general methods:

Attack Type	Description
Brute Force	In a brute force attack, the attacker tries every known combination. These types of attacks take the longest amount of time, though they are always successful if enough time is allowed. Cryptosystems are almost always subject to brute force attacks against the key. Types of brute force attacks include: ▪ A mathematical attack, which is an attack on a key containing a small data set. The smaller data set provides fewer combinations to decipher. A 40-bit encryption is considered weak and a 128-bit encryption is considered strong. The longer the key, the more combinations a brute force attack will require. ▪ A birthday attack is a brute force attack that focuses on hashing algorithms. The attacker hashes messages until two plaintext messages are found that produce the same hashed value. This type of attack is based on the statistic that there is more than a 50% chance that two out of 23 people in a room will have the same birthday. To match a selected day, 253 people would need to be in the room.
Plaintext	Types of plaintext attacks include: ▪ A chosen cipher text attack, in which the attacker produces cipher text and then sends it through a decryption process to see the resulting plaintext. ▪ A known plaintext attack, in which the attacker has seen the plaintext and the resulting cipher text. The attacker can make conclusions about the encrypting key and will have validation if the encrypting key is discovered. ▪ A chosen plaintext attack, in which the attacker chooses the plaintext to be encrypted. This can occur when a worker steps away from the computer and the attacker sends a message and captures the resulting ciphertext (this attack is also known as a lunchtime attack or midnight attack). The attacker can select plaintext that will produce clues to the encryption key used.
Analytic	An analytic attack uses an algebraic manipulation to reduce the complexity of the algorithm.
Weakness Exploitation	Attacks exploiting weaknesses in encryption include: ▪ A statistical attack exploits weaknesses in a cryptosystem, such as inability to produce random numbers or floating point errors. ▪ A dictionary attack uses known words and common variations. ▪ A weak key attack is an attack on an encrypted algorithm that contains keys with poorly decrypted ciphertext. ▪ An implementation attack exploits implementation weaknesses, such as in software, the protocol, or the encryption algorithm. ▪ A hybrid attack refers to the technique of adding appendages to known dictionary words. (For example, 1password, password07, or p@ssword1.)
Encryption	Encryption attack types include: ▪ A key clustering attack, in which the attacker decrypts an encoded message using a different key than was used during encryption. ▪ A replay attack, in which the attacker attempts to re-transmit encryption session keys in hopes of accessing the encrypted resource in a decrypted mode. ▪ A PKI attack, in which the attacker attempts to have a user accept a fake or spoofed PKI certificate. ▪ A side-channel attack, which is based on information gained from the physical implementation of a cryptosystem rather than theoretical weaknesses in the algorithms, such as the length of time required during encryption or decryption.
Man-in-the-Middle	In a man-in-the-middle attack, the attacker is able to read, insert, and modify messages between two parties without either party knowing that the link between them has been compromised.
Downgrade	A downgrade attack is often exploited through a man-in-the-middle attack. Security protocols that employ encryption may have different modes of operations. A downgrade attack convinces a protocol to disregard a high-quality mode of operation and use a lower-quality mode instead. For instance, a higher mode may require an encrypted connection, but a lower mode may use clear text. An example of this flaw was found in OpenSSL, which is an open-source implementation of the SSL and TLS protocols.

Use these countermeasures to strengthen the cryptosystem:

- Use strong passwords
- Implement strong cryptosystems with redundant ciphers
- Implement long key spaces