**Movie DRM (Digital right management)**

The movie industry has used a variety of DRM schemes over the years to stem the worldwide problem of movie piracy. Two of the major technologies used to protect mass-distributed media are as follows:

**Content Scrambling System (CSS)** Enforces playback and region restrictions on DVDs. This encryption scheme was broken with the release of a tool known as DeCSS that enabled the playback of CSS-protected content on Linux systems.

**Advanced Access Content System (AACS)** Protects the content stored on Blu-Ray and HD DVD media. Hackers have demonstrated attacks that retrieved AACS encryption keys and posted them on the Internet.

**Analytic Attack** This is an algebraic manipulation that attempts to reduce the complexity of the algorithm. Analytic attacks focus on the logic of the algorithm itself.

**Implementation Attack** This is a type of attack that exploits weaknesses in the implementation of a cryptography system. It focuses on exploiting the software code, not just errors and flaws but the methodology employed to program the encryption system.

**Statistical Attack** A statistical attack exploits statistical weaknesses in a cryptosystem, such as floating-point errors and inability to produce truly random numbers. Statistical attacks attempt to find a vulnerability in the hardware or operating system hosting the cryptography application.

**Brute Force** Brute-force attacks are quite straightforward. Such an attack attempts every possible valid combination for a key or password. They involve using massive amounts of processing power to methodically guess the key used to secure cryptographic communications

**Frequency Analysis and the Ciphertext Only Attack** In many cases, the only information you have at your disposal is the encrypted ciphertext message, a scenario known as the *ciphertext only attack*

**Known Plaintext** In the known plaintext attack, the attacker has a copy of the encrypted message along with the plaintext message used to generate the ciphertext (the copy). This knowledge greatly assists the attacker in breaking weaker codes.

**Chosen Ciphertext** In a chosen ciphertext attack, the attacker has **the ability to decrypt chosen portions** of the ciphertext message and use the decrypted portion of the message to discover the key

**Chosen Plaintext** In a chosen plaintext attack, the attacker has the ability **to encrypt plaintext messages of their choosing and can then analyze the ciphertext o**utput of the encryption algorithm.

**Meet in the Middle** Attackers might use a meet-in-the-middle attack to defeat encryption algorithms that use two rounds of encryption . In the meet-in-the-middle attack, the attacker uses a known plaintext message. The plain text is then encrypted using every possible key (k1), and the equivalent ciphertext is decrypted using all possible keys (k2). When a match is found, the corresponding pair (k1, k2) represents both portions of the double encryption. This type of attack generally takes only double the time necessary to break a single round of encryption

**Birthday** The birthday attack, also known as a *collision attack* or *reverse hash matching .* In this attack, the malicious individual seeks to substitute in a digitally signed communication a different message that produces the same message digest, thereby maintaining the validity of the original digital signature.

**Replay** The replay attack is used against cryptographic algorithms that don’t incorporate temporal protections. In this attack, the malicious individual intercepts an encrypted message between two parties (often a request for authentication) and then later “replays” the captured message to open a new session. This attack can be defeated by incorporating a time stamp and expiration period into each message.

**SHA-256 produces a 256-bit message digest using a 512-bit block size.**

**■ SHA-224 uses a truncated version of the SHA-256 hash to produce a 224-bit message digest using a 512-bit block size.**

**■ SHA-512 produces a 512-bit message digest using a 1,024-bit block size.**

**■ SHA-384 uses a truncated version of the SHA-512 hash to produce a 384-bit digest using a 1,024-bit block size.**

**Hash function -**In most cases, a message digest is 128 bits or larger . The input can be of any length.■ The output has a fixed length. The hash function is one-way . The hash function is collision free (meaning that it is extremely hard to find two messages that produce the same hash value..