Attacks on Symmetric Key

Attacks against encrypted information fall into three main categories. They are:

1. Key search, brute force attacks
2. Cryptanalysis
3. Systems-based attacks

Key Search (Brute Force) Attacks

The most straight-forward attack on an encrypted message is simply to attempt to decrypt the message with every possible key. Most of these attempts will fail. But one might work. At which point you can decrypt the message and any others that that key is used on.

There is no way to defend against a key search attack because there is no way to keep an attacker from trying to decrypt your message with every possible key. Key searches are not very efficient. If the chosen key is long enough, a key search attack is not even feasible. For example, with a 128 bit key and any conceivable computing technology, life on Earth will cease to exist long before even a single key is likely to be cracked.

Cryptanalysis

Most encryption algorithms can be defeated by using a combination of sophisticated mathematics and computing power. The results are that many encrypted messages can be deciphered without knowing the key. A skilled cryptanalyst can sometimes decipher encrypted text without even knowing the encryption algorithm.

A cryptanalytic attack can have two possible goals. The cryptanalyst might have ciphertext and want to discover the plaintext, or the cryptanalyst might have ciphertext and want to discover the encryption key that was used to encrypt the message. The following attacks are commonly used when the encryption algorithm is known. These may be applied to encrypted files or Internet traffic:

Known Plaintext Attack

In this type of attack the cryptanalyst has a block of plaintext and a corresponding block of ciphertext. The goal of a known plaintext attack is to determine the cryptographic key and possibly the algorithm which can then be used to decrypt other messages.

Chosen Plaintext Attack

The cryptanalyst has the subject of the attack unknowingly encrypt chosen blocks of data creating a result that the cryptanalyst can then analyze. The goal of a chosen plaintext attack is to determine the cryptographic key which can then be used to decrypt other messages.

Differential Cryptanalysis

This attack, which is a form of chosen plaintext attack, involves encrypting many texts that are only slightly different from one another and comparing the results.

Differential Fault Analysis

The attack works against cryptographic systems that are built in hardware. The device is subjected to environmental factors (heat, stress, radiation, etc) designed to coax the device into making mistakes during the encryption or decryption operation. These faults can be analyzed, and from them the device's internal state, including the encryption key or algorithm, can possibly be discovered.

Differential Power Analysis

This is another attack against cryptographic hardware, in particular smart cards. By observing the power that a smart card uses to encrypt a chosen block of data, it is possible to learn a little bit of information about the structure of the secret key. By subjecting the smart card to a number of specially chosen data blocks and carefully monitoring the power used, it is possible to determine the secret key.

Differential Timing Analysis

This attack is similar to differential power analysis except that the attacker carefully monitors the time that the smart card takes to perform the requested encryption operations.

Note: True cryptographic security lies in openness and peer review, not in algorithmic secrecy.

Systems Based Attack

Another way of breaking a code is to attack the cryptographic system that uses the cryptographic algorithm without actually attacking the algorithm itself.

Early TV Satellite System

One of the most spectacular cases of a systems-based attack was the VC-I video encryption algorithm that was used in early satellite TV systems. Satellite signals were encrypted with VC-I encryption as part of the satellite subscription for premium channels. For many years, video pirates sold decoder boxes that could intercept the transmission of keys and use them to decrypt the satellite TV signals. The video pirates would capture the encryption keys and update the receiver boxes of the satellite customers. This way the satellite customers could get the premium channels for free.

Netscape's SSL Implementation

Many of the early attacks against Netscape's implementation of SSL were actually attacks on Netscape Navigator's implementation, rather than on the SSL protocol itself. Researchers David Wagner and Ian Goldberg at the University of California at Berkeley discovered that Navigator's random number generator was not really random. It was possible for attackers to closely monitor the computer that Navigator was running on, predict the random number generator’s starting configuration, and determine the randomly chosen key using a fairly straightforward configuration.

Covert Channels

Covert channels are defined as any communication channel that can be exploited by a process to transfer information in a manner that violates the system’s security policy. If an attacker cannot decrypt email messages, she may be able to gain information by examining the message sender,