Known Plaintext Attack

In cryptography, the known plaintext attack, or KPA, is an attack based on having samples of both the plaintext and corresponding encrypted or ciphertext for that information available. This information is used to conduct an analysis of the data in order to determine the secret key used to encrypt and decrypt the information. Historical ciphers are very susceptible to the attack, while modern-day ciphers are less prone to being cracked using the method.

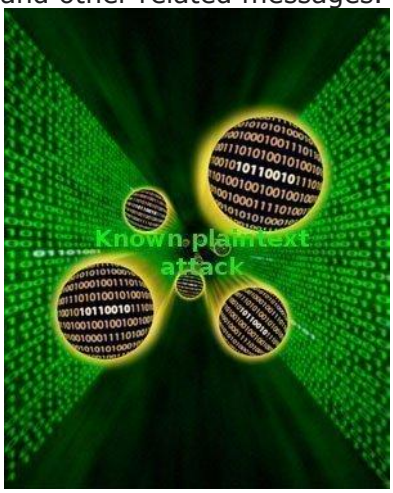
History of the Known Plaintext Attack

The history of the known plaintext attack dates to earlier in the 20th century when the cryptologists referred to the action using the term "crib." The term crib was based on the slang for using a "crib sheet" or "cheat sheet" on an exam. The general idea behind the original "cribs" was that if a cryptologist was able to obtain information regarding a word or phrase contained within ciphertext, that he or she would be able to have an advantage when creating a test to break into the cipher.

Without any intelligence advantage to develop the "crib," cryptologists were left to conduct random tests or attacks on the cipher to attempt to obtain common phrases within the ciphertext. Once the cribbed words would start to appear when conducting tests, the cryptologist(s) would know they were on the right track for breaking the cipher.

Breaking the Enigma Code

During WW II, the German military used the Enigma Machine for the encryption of military and other related messages. During this timeframe, the commanders were aware of the



potential threat of cribs to the code; however, the German operators in the field were not as conscious about maintaining OPSEC during the war. As a

result, British cryptologists were able to make a number of accurate guesses for establishing cribs due to the rigidity of the regimented German military report system. These cribs would typically be created based off of the German weather reports and other recurring information sent from the field to German high command. For example, the German world for weather, "Wetter," occurred in the same location in the same messages every day. Combined with knowing the actual weather conditions, the British cryptologists were able to make significant headway with cracking the Enigma code.

Another example of focusing on likely "known" transmissions by the German military to help crack the Enigma Code was in Africa during WW2. The German Afrika Corps would commonly send reports that stated "Nothing to Report," during the war. These transmissions along with other standard greetings allowed cryptographers working at Bletchley Park in the U.K. to make progress on breaking Enigma messages. Another tactic that the Allies would take to help obtain additional information for crib sheet development was to bomb or mine well-known areas. Once accomplished, the resulting Enigma messages transmitted by the Germans would contain references to set geographic positions. This act became to be known as "seeding" a given area.

Further helping the Allies develop crib sheets to aid in breaking the Enigma code was intelligence gleaned from the interrogation of a German intelligence operative. During this interview, it was ascertained that the German High Command had directed their message operators to spell out numbers to help to encode them. As a result, the now famous cryptology pioneer and computer scientist, Alan Turing, was able to conduct an analysis of decrypted Enigma messages. During this work, he was able to discover that the number "one" was the most common string of characters in the plaintext. He was then able to automate the crib process for the Allies creating the Eins catalog. This work assumed that "enis" (the German word for "one") was the most common string in any given plaintext. The work included all possible positions of the Enigma machine and keysettings.

Prior to World War 2, the Polish Cipher Bureau was able to exploit cribs when attempting to crack Enigma-encoded messages. During these pre-way exploits, the Polish engineers were able to take advantage of the Germans using the characters "ANX" throughout messages (AN is the German word for "to" and the character X was used as a spacer in the message), to develop cribs to decrypt messages.

How Good are Classic Ciphers?

Although classic ciphers worked wonders in their day, they are extremely vulnerable to the known plaintext attack with the technology of today. The Caesar cipher is able to be solved

with the attack using only a single letter of plaintext that is corroborated to ciphertext. For general monoalphabetic substitution ciphers, the known plaintext attack only needs several character pairs to quickly crack the cipher.

Modern Day Plaintext Attacks

One of the better known, modern-day plaintext attacks has been against the PKZIP stream cipher against older versions of the zip specification. If an attacker has a zip file encrypted under the older versions of PKZIP, he or she only needs to have part of one of the unencrypted files of the archive to conduct the attack. Freeware is published supporting the attack that is capable of calculating the private or secret key required to decrypt the full archive of information. In order to obtain the unencrypted file, an attacker simply has to search the website of the originating zip file to locate one that is suitable, manually construct a plaintext file using a filename from the archive, or locate the example file from another, related archive. This attack does not work against PKZIP files that have been encrypted using AES.

The Chosen Plaintext Attack

In the chosen plaintext attack, or CPA, the attacker has the ability or access to select random plaintexts and see the corresponding ciphertext. The ultimate goal of this attack is to obtain additional data or information that will reduce or eliminate the security of the cipher being employed. In the best case for the attacker (or worst case for the organization using the cipher), the secret key can be obtained which eliminates the overhead of cracking the cipher. In some instances of the chosen plaintext attack, only a small amount of plaintext must be known by the attacker. In these circumstances, the attack is known as a plaintext injection attack.

Although the chosen plaintext attack may at first appear to be an unrealistic model to leverage when trying to crack a cipher, it is primarily focused on leveraging software or computer hardware to obtain the data or information used in the attack. These attacks are more commonly used against public key cryptography where the attacker can obtain the public key easily and then generate ciphertext at will from a variety of plaintext source.

What are the Two Types of Chosen Plaintext Attack?

There are two types of chosen plaintext attack at the time of this writing: batch chosen plaintext attack and the adaptive chosen plaintext attack. In the batch chosen variant, the

analyst is able to select all plaintexts before they are encrypted. This version of the attack is often referred to by the generic chosen plaintext attack label. In the adaptive chosen plaintext attack, the attacker is able to conduct interactive queries of the cipher. Subsequent plaintext queries are able to be made based on the results of previous attempts. Through this progressive attack, the cryptanalyst is able to make more advanced headway on breaking the cipher. A related technique is the Allied "gardening" technique used during WW2. In this technique, the analysts were able to have the military take specific action that would be transmitted in encoded Enigma messages. Knowing the topic to expect in the resulting messages allowed the code breakers to make additional headway in cracking the Enigma code. Today, this variant of the attack is also known as the plaintext injection attack.

Chosen Ciphertext Attack

The chosen ciphertext attack, or CCA, is an attack based on the cryptanalyst obtaining information by selecting ciphertext and then obtaining the plaintext or decryption without knowing the key. To accomplish this attack, the cryptanalyst must be able to enter one to many ciphertexts into the cipher system and then obtain the resulting plain or cleartext. From this information, the secret key can be recovered for use in decryption.

The chosen ciphertext attack is able to defeat a number of secure cipher or security algorithms due to the ability of the attacker to be able to obtain plaintext on demand from the ciphertext. For example, the El Gamal cryptosystem is very secure against the chosen plaintext attack. Against the chosen ciphertext attack; however, the system is very unsecure. Additionally, early versions of RSA padding that were used in SSL were vulnerable to this attack and would reveal the SSL session keys. The attack has also been used to successfully target "tamper-resistant" smart cards. Since the card can come under the control of an attacker, a large number of chosen ciphertexts can be issued in an attempt to obtain the secret key used by the smart card.

If a cipher is susceptible to attack by the chosen ciphertext attack, the person or organization that implements the cipher has to be cautious and make sure situations are avoided that an attacker might be able to decrypt selected ciphertexts. Although this action seems simple to implement, even allowing partially chosen ciphertexts can allow various attacks to occur. Additionally, in cryptosystems that use the same cipher to encrypt and decrypt text are particularly susceptible to attack. In the cases where messages are not hashed as part of the encryption process, a better approach to use of the cipher is required for safe employment.

What are the Types of Chosen Ciphertext Attacks?

Similar to other types of cipher attack, chosen ciphertext attacks are either non-adaptive or adaptive. In the adaptive variants of the attack, the attacker selects the ciphertext based on results of previous plaintext to ciphertext decryptions. In non-adaptive attacks, the ciphertexts that will be decrypted are selected in advance. The resulting plaintext does not change the additional ciphertext look ups.

Lunchtime Attack

The lunchtime attack is a special variant of the chosen ciphertext attack. It is also referred to as the midnight, lunchtime, or indifferent attack. In this attack, the individual(s) are able to make adaptive queries on a crypto system up to a certain point that is very system dependent. On reaching this threshold, the attacker must be able to demonstrate an ability to attack the system.

The attack gets its name from the notion that an end-user's computer is open to attack while he or she is away from the desk at lunch time. If the attacker is able to make adaptive chosen ciphertext queries without limitation, no encrypted message is safe that uses the system until the access to make the attacks is removed. Once the ability to adapt queries is removed, the attack becomes known as being "non-adaptive."

Adaptive Chosen Ciphertext Attack

In the adaptive chosen chiphertext attack, ciphertext are able to be selected before and after a challenge ciphertext is provided to the attacker. The only limitation in the attack is that the challenge ciphertext is not able to be queried. This attack is considered to be stronger than a lunchtime attack and is also referred to as a CCA2 attack. There are very few non-academic attacks that take this format. Instead, the adaptive chosen cipherattack is used to test the security of a cipher against chosen ciphertext attacks. Some crypto systems that have been proved to be resistant to this type of attack include RSA-OAEP and the Cramer-Shoup system.

Source:

http://www.tech-faq.com/known-plaintext-attack.html