One-Time Pad

A one-time pad is a form of encryption that is difficult to decipher or crack if one is not the intended recipient. If done correctly, the strength of encryption of plaintext can almost be impossible to break in a useful timeframe. The system takes each character from plaintext and uses modular addition with a character from a pad or secret key of the same length of the plaintext to create ciphertext. If the key used to create the ciphertext is really random, as large or larger than the plaintext, never reused in any form, and kept truly secret, the ciphertext is unable to be decrypted in a usable timeframe. Although one-time pads are theoretically sound, there have been a number of practical implementation issues keeping the pads from seeing widespread use.

When was the One-Time Pad Discovered?

The one-time pad has been invented, an re-invented several times over the years. The technique was first described in 1882 by Frank Miller, and later "re-discovered in 1917" with a successful patent claim made a few years later. The current one-time pad concept is based on the Vernam cipher created by Gilbert Vernam and other co-workers. His cipher combined a message with a key that was read from a punch tape. In the original form of the cipher, the encoded messages could eventually be cracked since the key tape was setup on a loop that resulted in the key being reused making the cipher open to cryptanalysis. The "one-time" aspect of the cipher came into play a bit later when Joseph Mauborgne discovered the fact that if they key tape was fully random, cryptanalysis would be difficult if not impossible.

The pad aspect of the "One-Time Pad" name originated from the early implementations of the cipher where the key materials were given to personnel on a pad of paper. This was to allow the top sheet of the pad to be torn off and destroyed easily after use. Many times, the pad would be reduced to an extremely small size that would require the use of a magnifying glass to use it. Many times, one-time pads would be printed onto extremely flammable nitrocellulose paper to allow for easy disposal.

One-Time Pad History

Frank Miller is credited with first writing about and describing the one-time pad cryptography system in 1882. In 1917, Gilbert Vernam of the AT&T Corporation was the first to invent and patent an electrical one-time patent system in 1917 and 1919 respectfully based on existing teleprinter technology. Every character in a message in this discovery was combined electrically with a character located on a tape key in the device.

Then Captain Joseph Mauborgne, U.S. Army, was able to ascertain that if the character sequence on the tape was made completely random, the ability to crack the cipher text would be significantly more difficult. He would go on with Vernam to create the first one-time tape system for one-time pads.

The subsequent development in one-time pad history was the creation of the paper pad. For just about the length of modern history, diplomatic personnel had often used ciphers to maintain confidentiality when reporting back to their home country and to minimize the cost of telegraph transmissions. For these codes, words were converted to numbers using a codebook. To add more security, numbers could be combined with each code group along with using a secret number in a process referred to as superencryption. In the 1920s, three German scientists or cryptographers realized (Erich Langlotz, Rudolf Schauffler, and Werner Kunze) that these systems could not be broken if the number chosen to add to the system was picked at random for every code grouping. They would use duplicated paper pads that contained lines of random number groupings. Each of these pages would contain eight lines and a serial number with every line containing six, five-digit numbers on it. A page would then be used to encode a message and be subsequently destroyed. The serial number of the pad would be sent with the transmitted message to allow the recipient to reverse the message and destroy the copy of the page. The system was placed into operation by the German government in 1923.

The British also "invented" a variant of a one-time pad of letters used to encode plaintext directly. Their version was invented for use by the British Special Operations Executive during World War 2 and for use at Bletchley Park.

Finally, Claude Shannon proved the theoretical significance of the one-time pad in the 1940s. His work was published in a classified report in 1945 and later permitted to be openly published in 1949. In the same timeframe, Vladimir Kotelnikov was able to independently prove the security of the one-time pad in 1941; however, his work remains classified to this day.

Problems with the One-Time Pad

As Shannon proved, if everything works perfectly, the one-time pad is one of the strongest ciphers that are known today. The practice of implementing the one-time pad remains problematic. The first barrier is the requirement for the perfectly random keys which are not easy or cheap to produce. The keys have to be the same or longer length as the message being sent. The next challenge lies in the physical security of the one-time pad key. If an adversary is able to obtain copies of the key being used, or they are re-used in error, then the cipher's security can be called into question.

The security of a one-time pad fully lies in the physical security capabilities of the organization implementing the system. In the purely theoretical setting, a one-time pad is very difficult if not impossible to crack. In the real-world; however, the balance between convenience, ease-of-use, and implementation practices make it much easier for adversaries to break one-time pad systems. As a result, these challenges have significantly decreased the frequency that the system has been implemented since creation.
With the subsequent invention of high-quality ciphers in industry and government circles that do not rely as much on physical security of secret keys, one-time pads have become less popular. By addressing the ease-of-use concerns, the modern ciphers in use today such as public key cryptography have seen significant growth in use over the one-time pad.

One-Time Pad Key Distribution

One of the primary issues when implementing a one-time pad is creating a distribution system that is secure. Since the key must be as long or longer than the message, there are many cases where using the pad does not make sense if one can send the key securely to the person intending to transmit a message. If an extremely long pad has been securely delivered; however, it is able to be used for more than one message transmission until the sum of all messages is equivalent to the length or size of the pad.

Transmitting or distributing extremely long keys has its own problems. First, it can be inconvenient or costly to send a long key. Secondly, this poses a high security risk. Since the key has to be extremely long, it must be transmitted or transported in a physically

secure manner. If intercepted, copied, and allowed to be delivered, an adversary may be able to decrypt and read a large number of messages sent without the users of the system being aware that the messages are not secure.

Finally, the level of effort required to manage one-time pad secure keys does not scale easily for large networks. When attempting to implement the system over a large data set of users, the requirement for secure keys increases by the square of the total number of end-users requiring the encryption service. For small numbers of people or agents, the scaling issue is not a significant issue.

Also, the secure key material for the one-time pad must be deleted or disposed of after being used to encrypt information. The same key cannot be reused or the messages previously sent using the key can be decrypted by unauthorized personnel.

How are One-Time Pad Keys Authenticated?

As designed and traditionally used, one-time cipher pads do not provide a means of authentication. This leaves a significant hole in the security of the ciphertext produced by a pad and poses a potential vulnerability in the message integrity. If an attacker knows what the content of a message is supposed to be, then he or she can proceed with replacing information in the message. This type of vulnerability is known as malleability and is coming with stream ciphers.
Techniques employed to guard against this vulnerability include the use of a message authentication code, Russian copulation, and variable length padding. Universal hashing also provides another means to authenticate messages, but the technique requires the use of more random data from the pad and requires the use of a computer.

Importance of Randomness in One-Time Pad Keys

It is difficult to create high-quality random numbers. The majority of random number generator libraries in programming languages are not considered strong enough for professional cryptographic utilities. Those that are strong enough for daily use, make use of cryptographic functions / ciphers that have not had their strength validated mathematically, or are not strong enough for classified information.

If an organization has the resources to create strong random numbers for the secret key used by a one-time pad, a common mistake is to reuse components of a one-time pad. For example, if an adversary has access to the ciphertext produced by one-time pads and one

key is reused, the complexity of the cipher can be reduced to that equivalent of a running key cipher.

What are the Uses for One-Time Pads?

In the modern-age, any digital storage device (USB stick, iPod, iPhone, Android phone, CD/DVD, portable hard drive, etc) can be used to store and/or transport one-time pad information. Although the one-time padsystem has a number of physical security barriers to effective use, it continues to have practical interest in scenarios where a computation by hand is useful for a given situation in intelligence circles. In these cases, pads can be delivered by hand via a "handler" or centralized point of contact to agents in the field, or via secure phone or computer connection.

The cipher technique has also proved useful in cases where two people work in a secure environment and one must travel to a less secure location for work. In this case, the person traveling can take the one-time pad with them on the road and minimize the risk of interception of the pad by an adversary. Other uses of the pad include: superencryption, quantum key distribution, and in educational contexts.

Historical Uses of the One-Time Pad

Since the early 1900s, one-time pads have been used by diplomatic services throughout the world. In the early 1920s, the Weimar Republic Diplomatic Service commenced using the method. In this same timeframe, the Soviet Union suffered several embarrassing cases of encrypted messages being made public and adopted the use of the pads in the 1930s. The Soviet KGB continued to use the method throughout the early Cold War with several cases of agents such as Colonel Rudolf Abel and the Krogers being arrested in the 1950s and 1960s with one-time pads in their possession.

During World War II, the British Special Operations Executive leveraged one-time-pads to encode message traffic sent between the agency's offices. Agent use of the system was introduced later in the war along with one-time tape cipher machines (Noreen and Rockex). One-time tape systems 5-UCO and SIGTOT were introduced by the United States NSA for use in sending and receiving intelligence traffic. The KW-26 electronic cipher was introduced in 1957 for use by the United States intelligence agencies.

The UK Army uses the BATCO tactical communications code that is based on a one-time pad system using pencil and paper. Key material is provided on paper sheets that are kept in a plastic wallet that uses a sliding indicator to show the last key used in the pad. When

deployed in the field, new sheets for the codebook are provided daily, and used on voice nets. When transmitted via voice, ciphertext is verbally read over the net.

Historical Exploits of the One-Time Pad

Although one-time pads are theoretically secure, mistakes in the physical security aspects of the pad's use can provide adversaries significant advantages in decrypting supposedly secure traffic. In the later portions of WW2, the United States Army Signals Intelligence Service was able to crack the German Foreign Office's high-level traffic system, GEE. The American analysts were able to determine that the keys used for the pads were not completely random due to the machine used for key generation creating predictable outputs.

In 1945, the Americans were able to discover Canberra-Moscow messages that were encrypted using a code book and one-time pad. The one-time pad was the same one used for messages sent from Moscow to Washington, D.C. Since many of the messages included known U.K. government documents, analysts were able to decrypt many of the messages that were sent.

During WW2 and throughout the Cold War, Soviet spy agencies made heavy use of one-time pads for communications with agent controllers and field agents. Many of the pads were created by typists on type writers, which although not purely random, proved effective against analysis. Without obtaining copies of the key materials, Allied powers had a difficult time attempting to crack the ciphertext used in these communications.

In the late 1940s; however, both British and the American intelligence agencies were able to break a significant amount of the Soviet one-time pad message traffic sent to Moscow during WW2. This breakthrough came as a result of a number of errors the Soviets made while creating and distributing key material. Some of these mistakes included making more than one copy of the same key material during the timeframe that German forces were invading the Soviet Union. The effort in cracking the Soviet code was named VENONA which produced a significant amount of intelligence regarding Soviet spy efforts against the Allies during the War.

Source:

http://www.tech-faq.com/one-time-pad.html