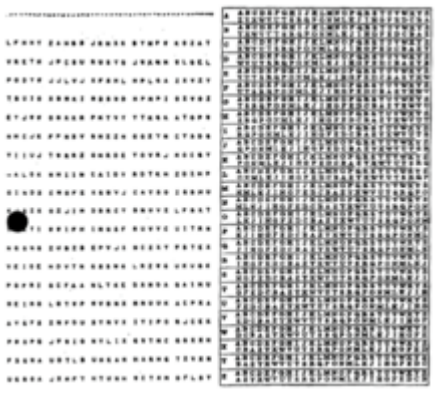
One-time pad

In cryptography, the **one-time pad** (**OTP**) is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key the same size as, or longer than, the message being sent. In this technique, a plaintext is paired with a random secret key (also referred to as *a one-time pad*). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is (1) truly random, (2) at least as long as the plaintext, (3) never reused in whole or in part, and (4) kept completely secret, then the resulting ciphertext will be impossible to decrypt or break.[1][2] It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys.[3] Digital versions of one-time pad ciphers have been used by nations for some critical diplomatic and military communication, but the problems of secure key distribution have made them impractical for most applications.



A format of one-time pad used by the U.S. National Security Agency, code named DIANA. The table on the right is an aid for converting between plaintext and ciphertext using the characters at left as the key.

First described by Frank Miller in 1882,[4][5] the one-time pad was re-invented in 1917. On July 22, 1919, U.S. Patent 1,310,719 was issued to Gilbert S. Vernam for the XOR operation used for the encryption of a one-time pad.[6] Derived from his *Vernam cipher*, the system was a cipher that combined a message with a key read from a punched tape. In its original form, Vernam's system was vulnerable because the key tape was a loop, which was reused whenever the loop made a full cycle. One-time use came later, when Joseph Mauborgne recognized that if the key tape were totally random, then cryptanalysis would be impossible.[7]

The "pad" part of the name comes from early implementations where the key material was distributed as a pad of paper, so that the top sheet could be easily torn off and destroyed after use. For ease of concealment, the pad was sometimes reduced to such a small size that a powerful magnifying glass was required to use it. The KGB used pads of such size that they could fit in the palm of a hand,[8] or in a walnut shell.[9] To increase security, one-time pads were sometimes printed onto sheets of highly flammable nitrocellulose, so that they could be quickly burned after use.

There is some ambiguity to the term "Vernam cipher" because some sources use "Vernam cipher" and "one-time pad" synonymously, while others refer to any additive stream cipher as a "Vernam cipher", including those based on a cryptographically secure pseudorandom number generator (CSPRNG).[10]

Contents

History

Frank Miller in 1882 was the first to describe the one-time pad system for securing telegraphy.[5][11]

The next one-time pad system was electrical. In 1917, Gilbert Vernam (of AT&T Corporation) invented and later patented in 1919 (U.S. Patent 1,310,719 (https://www.google.com/patents/US1310719)) a cipher based on teleprinter technology. Each character in a message was electrically combined with a character on a punched paper tape key. Joseph Mauborgne (then a captain in the U.S. Army and later chief of the Signal Corps) recognized that the character sequence on the key tape could be completely random and that, if so, cryptanalysis would be more difficult. Together they invented the first one-time tape system.[10]

The next development was the paper pad system. Diplomats had long used codes and ciphers for confidentiality and to minimize telegraph costs. For the codes, words and phrases were converted to groups of numbers (typically 4 or 5 digits) using a dictionary-like codebook. For added security, secret numbers could be combined with (usually modular addition) each code group before transmission, with the secret numbers being changed periodically (this was called superencryption). In the early 1920s, three German cryptographers (Werner Kunze, Rudolf Schauffler and Erich Langlotz), who were involved in breaking such systems, realized that they could never be broken if a separate randomly chosen additive number was used for every code group. They had duplicate paper pads printed with lines of random number groups. Each page had a serial number and eight lines. Each line had six 5-digit numbers. A page would be used as a work sheet to encode a message and then destroyed. The serial number of the page would be sent with the encoded message. The recipient would reverse the procedure and then destroy his copy of the page. The German foreign office put this system into operation by 1923.[10]

A separate notion was the use of a one-time pad of letters to encode plaintext directly as in the example below. Leo Marks describes inventing such a system for the British Special Operations Executive during World War II, though he suspected at the time that it was already known in the highly compartmentalized world of cryptography, as for instance at Bletchley Park.[12]

The final discovery was made by information theorist Claude Shannon in the 1940s who recognized and proved the theoretical significance of the one-time pad system. Shannon delivered his results in a classified report in 1945, and published them openly in 1949.[3] At the same time, Soviet information theorist Vladimir Kotelnikov had independently proved absolute security of the one-time pad; his results were delivered in 1941 in a report that apparently remains classified.[13]

Example

Suppose Alice wishes to send the message "HELLO" to Bob. Assume two pads of paper containing identical random sequences of letters were somehow previously produced and securely issued to both. Alice chooses the appropriate unused page from the pad. The way to do this is normally arranged for in advance, as for instance 'use the 12th sheet on 1 May', or 'use the next available sheet for the next message'.

The material on the selected sheet is the *key* for this message. Each letter from the pad will be combined in a predetermined way with one letter of the message. (It is common, but not required, to assign each letter a numerical value, e.g., "A" is 0, "B" is 1, and so on.)

In this example, the technique is to combine the key and the message using modular addition. The numerical values of corresponding message and key letters are added together, modulo 26. So, if key material begins with "XMCKL" and the message is "HELLO", then the coding would be done as follows:

```
     H       E       L       L       O  message
  7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= 30      16      13      21      25     message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) (message + key) mod 26
     E       Q       N       V       Z  → ciphertext
```

If a number is larger than 26, then the remainder after subtraction of 26 is taken in modular arithmetic fashion. This simply means that if the computations "go past" Z, the sequence starts again at A.

The ciphertext to be sent to Bob is thus "EQNVZ". Bob uses the matching key page and the same process, but in reverse, to obtain the plaintext. Here the key is *subtracted* from the ciphertext, again using modular arithmetic:

```
     E       Q       N       V       Z  ciphertext
   4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= -19       4      11      11      14     ciphertext − key
=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) ciphertext − key (mod 26)
      H       E       L       L       O  → message
```

Similar to the above, if a number is negative then 26 is added to make the number zero or higher.

Thus Bob recovers Alice's plaintext, the message "HELLO". Both Alice and Bob destroy the key sheet immediately after use, thus preventing reuse and an attack against the cipher. The KGB often issued its agents one-time pads printed on tiny sheets of "flash paper"—paper chemically converted to nitrocellulose, which burns almost instantly and leaves no ash.[14]

The classical one-time pad of espionage used actual pads of minuscule, easily concealed paper, a sharp pencil, and some mental arithmetic. The method can be implemented now as a software program, using data files as input (plaintext), output (ciphertext) and key material (the required random sequence). The XOR operation is often used to combine the plaintext and the key elements, and is especially attractive on computers since it is usually a native machine instruction and is therefore very fast. It is, however, difficult to ensure that the key material is actually random, is used only once, never becomes known to the opposition, and is completely destroyed after use. The auxiliary parts of a software one-time pad implementation present real challenges: secure handling/transmission of plaintext, truly random keys, and one-time-only use of the key.

Attempt at cryptanalysis

To continue the example from above, suppose Eve intercepts Alice's ciphertext: "EQNVZ". If Eve had infinite time, she would find that the key "XMCKL" would produce the plaintext "HELLO", but she would also find that the key "TQURI" would produce the plaintext "LATER", an equally plausible message:

```
   4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-  19 (T)  16 (Q)  20 (U)  17 (R)   8 (I) possible key
= −15       0      −7       4      17     ciphertext-key
=  11 (L)   0 (A)  19 (T)   4 (E)  17 (R) ciphertext-key (mod 26)
```

In fact, it is possible to "decrypt" out of the ciphertext any message whatsoever with the same number of characters, simply by using a different key, and there is no information in the ciphertext that will allow Eve to choose among the various possible readings of the ciphertext.

Perfect secrecy

One-time pads are "information-theoretically secure" in that the encrypted message (i.e., the ciphertext) provides no information about the original message to a cryptanalyst (except the maximum possible length[15] of the message). This is a very strong notion of security first developed during WWII by Claude Shannon and proved, mathematically, to be true for the one-time pad by Shannon about the same time. His result was published in the *Bell Labs Technical Journal* in 1949.[16] Properly used, one-time pads are secure in this sense even against adversaries with infinite computational power.

Claude Shannon proved, using information theory considerations, that the one-time pad has a property he termed *perfect secrecy*; that is, the ciphertext *C* gives absolutely no additional information about the plaintext.[note 1] This is because, given a truly random key that is used only once, a ciphertext can be translated into *any* plaintext of the same length, and all are equally likely. Thus, the *a priori* probability of a plaintext message *M* is the same as the *a posteriori* probability of a plaintext message *M* given the corresponding ciphertext.

Mathematically, this is expressed as $\mathbf{H}(M) = \mathbf{H}(M|C)$, where $\mathbf{H}(M)$ is the information entropy of the plaintext and $\mathbf{H}(M|C)$ is the conditional entropy of the plaintext given the ciphertext *C*. (Here, '*H*' is the capital greek letter eta.) This implies that for every message *M* and corresponding ciphertext *C*, there must be at least one key *K* that binds them as a one-time pad. Mathematically speaking, this means $K \geq C \geq M$, where K, C, M denotes the distinct quantity of keys, ciphers and messages. In other words, if you need to be able to go from any plaintext in message space *M* to any cipher in cipher-space *C* (encryption) and from any cipher in cipher-space *C* to a plain text in message space *M* (decryption), you need at least $|M| = |C|$ keys (all keys used with equal probability of $1/|K|$ to ensure perfect secrecy).

Another way of stating perfect secrecy is based on the idea that for all messages m_1, m_2 in message space *M*, and for all ciphers *c* in cipher space *C*, we have $\Pr_{k \Leftarrow \mathbf{K}}[E_k(m_1) = c] = \Pr_{k \Leftarrow \mathbf{K}}[E_k(m_2) = c]$, where $\Pr$ represents the probabilities, taken over a choice of k in key space $\mathbf{K}$ over the coin tosses of a probabilistic algorithm, E. Perfect secrecy is a strong notion of cryptanalytic difficulty.[3]

Conventional symmetric encryption algorithms use complex patterns of substitution and transpositions. For the best of these currently in use, it is not known whether there can be a cryptanalytic procedure that can reverse (or, usefully, partially reverse) these transformations without knowing the key used during encryption. Asymmetric encryption algorithms depend on mathematical problems that are thought to be difficult to solve, such as integer factorization and discrete logarithms. However, there is no proof that these problems are hard, and a

mathematical breakthrough could make existing systems vulnerable to attack.[note 2]

Given perfect secrecy, in contrast to conventional symmetric encryption, OTP is immune even to brute-force attacks. Trying all keys simply yields all plaintexts, all equally likely to be the actual plaintext. Even with known plaintext, like part of the message being known, brute-force attacks cannot be used, since an attacker is unable to gain any information about the parts of the key needed to decrypt the rest of the message. The parts that are known will reveal *only* the parts of the key corresponding to them, and they correspond on a strictly one-to-one basis; no part of the key is dependent on any other part.

Problems

Despite Shannon's proof of its security, the one-time pad has serious drawbacks in practice because it requires:

- Truly random, as opposed to *pseudorandom*, one-time pad values, which is a non-trivial requirement. See pseudorandom number generator and random number generation.
  - True random number generators exist, but are typically slower and more specialized.
- Secure generation and exchange of the one-time pad values, which must be at least as long as the message.
  - The security of the one-time pad is only as secure as the security of the one-time pad exchange, because if an attacker is able to intercept the one-time pad value and know it is a one-time pad, they can decrypt the one-time pad's message.
- Careful treatment to make sure that the one-time pad values continue to remain secret, and are disposed of correctly preventing any reuse in whole or part—hence "one time". See data remanence for a discussion of difficulties in completely erasing computer media.

One-time pads solve few current practical problems in cryptography. High quality ciphers are widely available and their security is not considered a major worry at present.[17] Such ciphers are almost always easier to employ than one-time pads; the amount of key material that must be properly generated and securely distributed is far smaller, and public key cryptography overcomes this problem.[18]

Quantum computers have been shown by Peter Shor and others to be much faster at solving some of the difficult problems that grant asymmetric encryption its security. If quantum computers are built with enough qubits, and overcoming some limitations to error-correction; traditional public key cryptography will become obsolete. One-time pads, however, will remain secure. See quantum cryptography and post-quantum cryptography for further discussion of the ramifications of quantum computers to information security.

True randomness

High-quality random numbers are difficult to generate. The random number generation functions in most programming language libraries are not suitable for cryptographic use. Even those generators that are suitable for normal cryptographic use, including /dev/random and many hardware random number generators, may make some use of cryptographic functions whose security has not been proven. An example of how true randomness can be achieved is by measuring radioactive emissions.[19]

In particular, one-time use is absolutely necessary. If a one-time pad is used just twice, simple mathematical operations can reduce it to a running key cipher. If both plaintexts are in a natural language (e.g., English or Russian) then, even though both are secret, each stands a very high chance of being recovered by heuristic cryptanalysis, with possibly a few ambiguities. Of course, a longer message can only be broken for the portion that overlaps a shorter message, plus perhaps a little more by completing a word or phrase. The most famous exploit of this vulnerability occurred with the Venona project.[20]

Key distribution

Because the pad, like all shared secrets, must be passed and kept secure, and the pad has to be at least as long as the message, there is often no point in using one-time padding, as one can simply send the plain text instead of the pad (as both can be the same size and have to be sent securely). However, once a very long pad has been securely sent (e.g., a computer disk full of random data), it can be used for numerous future messages, until the sum of their sizes equals the size of the pad. Quantum key distribution also proposes a solution to this problem, assuming fault-tolerant quantum computers.

Distributing very long one-time pad keys is inconvenient and usually poses a significant security risk.[1] The pad is essentially the encryption key, but unlike keys for modern ciphers, it must be extremely long and is much too difficult for humans to remember. Storage media such as thumb drives, DVD-Rs or personal digital audio players can be used to carry a very large one-time-pad from place to place in a non-suspicious way, but even so the need to transport the pad physically is a burden compared to the key negotiation protocols of a modern public-key cryptosystem, and such media cannot reliably be erased securely by any means short of physical destruction (e.g., incineration). A 4.7 GB DVD-R full of one-time-pad data, if shredded into particles 1 1 mm^2 (0.0016 sq in) in size, leaves over 4 megabits of (admittedly hard to recover, but not impossibly so) data on each particle. In addition, the risk of compromise during transit (for example, a pickpocket swiping, copying and replacing the pad) is likely to be much greater in practice than the likelihood of compromise for a cipher such as AES. Finally, the effort needed to manage one-time pad key material scales very badly for large networks of communicants—the number of pads required goes up as the square of the number of users freely exchanging messages. For communication between only two persons, or a star network topology, this is less of a problem.

The key material must be securely disposed of after use, to ensure the key material is never reused and to protect the messages sent.[1] Because the key material must be transported from one endpoint to another, and persist until the message is sent or received, it can be more vulnerable to forensic recovery than the transient plaintext it protects (see data remanence).

Authentication

As traditionally used, one-time pads provide no message authentication, the lack of which can pose a security threat in real-world systems. For example, an attacker who knows that the message contains "meet jane and me tomorrow at three thirty pm" can derive the corresponding codes of the pad directly from the two known elements (the encrypted text and the known plaintext). The attacker can then replace that text by any other text of exactly the same length, such as "three thirty meeting is canceled, stay home." The attacker's knowledge of the one-time pad is limited to this byte length, which must be maintained for any other content of the message to remain valid. This is a little different from malleability[21] where it is not taken necessarily that the plaintext is known. *See also* stream cipher attack.

Standard techniques to prevent this, such as the use of a message authentication code can be used along with a one-time pad system to prevent such attacks, as can classical methods such as variable length padding and Russian copulation, but they all lack the perfect security the OTP itself has. Universal hashing provides a way to authenticate messages up to an arbitrary security bound (i.e., for any $p > 0$, a large enough hash ensures that even a computationally unbounded attacker's likelihood of successful forgery is less than p), but this uses additional random data from the pad, and removes the possibility of implementing the system without a computer.

Uses

Applicability

Despite its problems, the one-time-pad retains some practical interest. In some hypothetical espionage situations, the one-time pad might be useful because it can be computed by hand with only pencil and paper. Indeed, nearly all other high quality ciphers are entirely impractical without computers. Spies can receive their pads in person from their "handlers." In the modern world, however, computers (such as those embedded in personal electronic devices such as mobile phones) are so ubiquitous that possessing a computer suitable for performing conventional encryption (for example, a phone that can run concealed cryptographic software) will usually not attract suspicion.

- The one-time-pad is the optimum cryptosystem with theoretically perfect secrecy.
- The one-time-pad is one of the most practical methods of encryption where one or both parties must do all work by hand, without the aid of a computer. This made it important in the pre-computer era, and it could conceivably still be useful in situations where possession of a computer is illegal or incriminating or where trustworthy computers are not available.
- One-time pads are practical in situations where two parties in a secure environment must be able to depart from one another and communicate from two separate secure environments with perfect secrecy.
- The one-time-pad can be used in superencryption.[22]
- The algorithm most commonly associated with quantum key distribution is the one-time pad.
- The one-time pad is mimicked by stream ciphers.
- The one-time pad can be a part of an introduction to cryptography.[23]

Historical uses

One-time pads have been used in special circumstances since the early 1900s. In 1923, it was employed for diplomatic communications by the German diplomatic establishment.[24] The Weimar Republic Diplomatic Service began using the method in about 1920. The breaking of poor Soviet cryptography by the British, with messages made public for political reasons in two instances in the 1920s (ARCOS case), appear to have induced the U.S.S.R. to adopt one-time pads for some purposes by around 1930. KGB spies are also known to have used pencil and paper one-time pads more recently. Examples include Colonel Rudolf Abel, who was arrested and convicted in New York City in the 1950s, and the 'Krogers' (i.e., Morris and Lona Cohen), who were arrested and convicted of espionage in the United Kingdom in the early 1960s. Both were found with physical one-time pads in their possession.

A number of nations have used one-time pad systems for their sensitive traffic. Leo Marks reports that the British Special Operations Executive used one-time pads in World War II to encode traffic between its offices. One-time pads for use with its overseas agents were introduced late in the war.[12] A few British one-time tape cipher machines include the Rockex and Noreen. The German Stasi Sprach Machine was also capable of using one time tape that East Germany, Russia, and even Cuba used to send encrypted messages to their agents.[25]

The World War II voice scrambler SIGSALY was also a form of one-time system. It added noise to the signal at one end and removed it at the other end. The noise was distributed to the channel ends in the form of large shellac records that were manufactured in unique pairs. There were both starting synchronization and longer-term phase drift problems that arose and were solved before the system could be used.

The hotline between Moscow and Washington D.C., established in 1963 after the Cuban missile crisis, used teleprinters protected by a commercial one-time tape system. Each country prepared the keying tapes used to encode its messages and delivered them via their embassy in the other country. A unique advantage of the OTP in this case was that neither country had to reveal more sensitive encryption methods to the other.[26]

U.S. Army Special Forces used one-time pads in Vietnam. By using Morse code with one-time pads and continuous wave radio transmission (the carrier for Morse code), they achieved both secrecy and reliable communications.

During the 1983 Invasion of Grenada, U.S. forces found a supply of pairs of one-time pad books in a Cuban warehouse.[27]

Starting in 1988, the African National Congress (ANC) used disk-based one-time pads as part of a secure communication system between ANC leaders outside South Africa and in-country operatives as part of Operation Vula, a successful effort to build a resistance network inside South Africa. Random numbers on the disk were erased after use. A Belgian airline stewardess acted as courier to bring in the pad disks. A regular resupply of new disks was needed as they were used up fairly quickly. One problem with the system was that it could not be used for secure data storage. Later Vula added a stream cipher keyed by book codes to solve this problem.[28]

A related notion is the one-time code—a signal, used only once, e.g., "Alpha" for "mission completed", "Bravo" for "mission failed" or even "Torch" for "Allied invasion of French Northern Africa"[29] cannot be "decrypted" in any reasonable sense of the word. Understanding the message will require additional information, often 'depth' of repetition, or some traffic analysis. However, such strategies (though often used by real operatives, and baseball coaches) are not a cryptographic one-time pad in any significant sense.

NSA

At least into the 1970s, the U.S. National Security Agency (NSA) produced a variety of manual one-time pads, both general purpose and specialized, with 86,000 one-time pads produced in fiscal year 1972. Special purpose pads were produced for what NSA called "pro forma" systems, where “the basic framework, form or format of every message text is identical or nearly so; the same kind of information, message after message, is to be presented in the same order, and only specific values, like numbers, change with each message.” Examples included nuclear launch messages and radio direction finding reports (COMUS).[30]:pp. 16–18

General purpose pads were produced in several formats, a simple list of random letters (DIANA) or just numbers (CALYPSO), tiny pads for covert agents (MICKEY MOUSE), and pads designed for more rapid encoding of short messages, at the cost of lower density. One example, ORION, had 50 rows of plaintext alphabets on one side and the corresponding random cipher text letters on the other side. By placing a sheet on top of a piece of carbon paper with the carbon face up, one could circle one letter in each row on one side and the corresponding letter one the other side would be circled by the carbon paper. Thus one ORION sheet could quickly encode or decode a message up to 50 characters long. Production of ORION pads required printing both sides in exact registration, a difficult process, so NSA switched to another pad format, MEDEA, with 25 rows of paired alphabets and random characters. (*See* Commons:Category:NSA one-time pads for illustrations.)

The NSA also built automated systems for the “centralized headquarters of CIA and Special Forces units so that they can efficiently process the many separate one-time pad messages to and from individual pad holders in the field.”[30]:pp. 21–26

During World War II and into the 1950s, the U.S. made extensive use of one-time tape systems. In addition to providing confidentiality, circuits secured by one-time tape ran continually, even when there was no traffic, thus protecting against traffic analysis. In 1955, NSA produced some 1,660,000 rolls of one time tape. Each roll was 8 inches in diameter, contained 100,000 characters, lasted 166 minutes and cost $4.55 to produce. By 1972, only 55,000 rolls were produced, as one-time tapes were replaced by rotor machines such as SIGTOT, and later by electronic devices based on shift registers.[30]:pp. 39–44 The NSA describes one-time tape systems like 5-UCO and SIGTOT as being used for intelligence traffic until the introduction of the electronic cipher based KW-26 in 1957.[31]

Exploits

While one-time pads provide perfect secrecy if generated and used properly, small mistakes can lead to successful cryptanalysis:

- In 1944–1945, the U.S. Army's Signals Intelligence Service was able to solve a one-time pad system used by the German Foreign Office for its high-level traffic, codenamed GEE.[32] GEE was insecure because the pads were not sufficiently random—the machine used to generate the pads produced predictable output.
- In 1945, the US discovered that Canberra–Moscow messages were being encrypted first using a code-book and then using a one-time pad. However, the one-time pad used was the same one used by Moscow for Washington, D.C.–Moscow messages. Combined with the fact that some of the Canberra–Moscow messages included known British government documents, this allowed some of the encrypted messages to be broken.
- One-time pads were employed by Soviet espionage agencies for covert communications with agents and agent controllers. Analysis has shown that these pads were generated by typists using actual typewriters. This method is of course not truly random, as it makes certain convenient key sequences more likely than others, yet it proved to be generally effective because while a person will not produce truly random sequences they equally do not follow the same kind of structured mathematical rules that a machine would either, and each person generates ciphers in a different way making attacking any message challenging. Without copies of the key material used, only some defect in the generation method or reuse of keys offered much hope of cryptanalysis. Beginning in the late 1940s, US and UK intelligence agencies were able to break some of the Soviet one-time pad traffic to Moscow during WWII as a result of errors made in generating and distributing the key material. One suggestion is that Moscow Centre personnel were somewhat rushed by the presence of German troops just outside Moscow in late 1941 and early 1942, and they produced more than one copy of the same key material during that period. This decades-long effort was finally codenamed VENONA (BRIDE had been an earlier name); it produced a considerable amount of information, including more than a little about some of the Soviet atom spies. Even so, only a small percentage of the intercepted messages were either fully or partially decrypted (a few thousand out of several hundred thousand).[33]
- The one-time tape systems used by the U.S. employed electromechanical mixers to combine bits from the message and the one-time tape. These mixers radiated considerable electromagnetic energy that could be picked up by an adversary at some distance from the encryption equipment. This effect, first noticed by Bell Labs during World War II, could allow interception and recovery of the plaintext of messages being transmitted, a vulnerability code-named Tempest.[30]:pp. 89 ff

See also

- *Agrippa (A Book of the Dead)*
- Information theoretic security
- Numbers station
- One-time password
- Session key
- Steganography
- Tradecraft
- Unicity distance

Notes

1. That is to say, the "**information gain**" or Kullback–Leibler divergence of the plaintext message from the cyphertext message is zero.
2. Most asymmetric encryption algorithms rely on the facts that the best known algorithms for prime factorization and computing discrete logarithms are superpolynomial time. There is a strong belief that these problems are not solvable by a Turing machine in time that scales polynomially with input length, rendering them difficult (hopefully, prohibitively so) to be broken via cryptographic attacks. However, this has not been proven.

References

1. "Intro to Numbers Stations" (https://web.archive.org/web/20141018031055/http://www.numbers-stations.com/intro). Archived from the original (http://www.numbers-stations.com/intro) on 18 October 2014. Retrieved 13 September 2014.
2. "One-Time Pad (OTP)" (https://web.archive.org/web/20140314175211/http://www.cryptomuseum.com/crypto/otp.htm). Cryptomuseum.com. Archived from the original (http://www.cryptomuseum.com/crypto/otp.htm) on 2014-03-14. Retrieved 2014-03-17.
3. Shannon, Claude (1949). "Communication Theory of Secrecy Systems". *Bell System Technical Journal*. **28** (4): 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x (https://doi.org/10.1002%2Fj.1538-7305.1949.tb00928.x).
4. Miller, Frank (1882). *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. C.M. Cornwell.
5. Bellovin, Steven M. (2011). "Frank Miller: Inventor of the One-Time Pad". *Cryptologia*. **35** (3): 203–222. doi:10.1080/01611194.2011.583711 (https://doi.org/10.1080%2F01611194.2011.583711). ISSN 0161-1194 (https://www.worldcat.org/issn/0161-1194).
6. "'Secret signaling system patent' on Google.Com" (http://www.google.com/patents/US1310719). *google.com*. Archived (https://web.archive.org/web/20160311030400/http://www.google.com/patents/US1310719) from the original on 11 March 2016. Retrieved 3 February 2016.
7. Kahn, David (1996). *The Codebreakers*. Macmillan. pp. 397–8. ISBN 978-0-684-83130-5.
8. "One-Time-Pad (Vernam's Cipher) Frequently Asked Questions, with photo" (http://www.ranum.com/security/computer_security/papers/otp-faq). Archived (https://web.archive.org/web/20060507212354/http://www.ranum.com/security/computer_security/papers/otp-faq/) from the original on 2006-05-07. Retrieved 2006-05-12.
9. Savory, Stuart (2001). "Chiffriergerätebau : One-Time-Pad, with photo" (http://users.telenet.be/d.rijmenants/pics/otpbooklet1.jpg) (in German). Archived (https://web.archive.org/web/20110530202013/http://users.telenet.be/d.rijmenants/pics/otpbooklet1.jpg) from the original on 2011-05-30. Retrieved 2006-07-24.
10. Kahn, David (1967). *The Codebreakers*. Macmillan. pp. 398 ff. ISBN 978-0-684-83130-5.
11. John Markoff (July 25, 2011). "Codebook Shows an Encryption Form Dates Back to Telegraphs" (https://www.nytimes.com/2011/07/26/science/26code.html?ref=science). *The New York Times*. Archived (https://web.archive.org/web/20130521201312/http://www.nytimes.com/2011/07/26/science/26code.html?ref=science) from the original on May 21, 2013. Retrieved 2011-07-26.
12. Marks, Leo (1998). *Between Silk and Cyanide: a Codemaker's Story, 1941-1945*. HarperCollins. ISBN 978-0-684-86780-9.
13. Sergei N Molotkov (Institute of Solid-State Physics, Russian Academy of Sciences, Chernogolovka, Moscow region, Russian Federation) (22 February 2006). "Quantum cryptography and V A Kotel'nikov's one-time key and sampling theorems" (http://www.turpion.org/php/paper.phtml?journal_id=pu&paper_id=6050). *Physics-Uspekhi*. **49** (7): 750–761. Bibcode:2006PhyU...49..750M (http://adsabs.harvard.edu/abs/2006PhyU...49..750M). doi:10.1070/PU2006v049n07ABEH006050 (https://doi.org/10.1070%2FPU2006v049n07ABEH006050). Retrieved 2009-05-03. PACS numbers: 01.10.Fv, 03.67.Dd, 89.70.+c and openly in Russian Квантовая криптография и теоремы В.А. Котельникова об одноразовых ключах и об отсчетах. УФН (http://www.ufn.ru/ru/articles/2006/7/k/)
14. Robert Wallace and H. Keith Melton, with Henry R. Schlesinger (2008). *Spycraft: The Secret History of the CIA's Spytechs, from Communism to al-Qaeda*. New York: Dutton. p. 452. ISBN 978-0-525-94980-0.
15. The actual length of a plaintext message can hidden by the addition of extraneous parts, called padding. For instance, a 21-character ciphertext could conceal a 5-character message with some padding convention (e.g. "-PADDING-HELLO -XYZ-") as much as an actual 21-character message: an observer can thus only deduce the maximum possible length of the significant text, not its exact length.
16. Shannon, Claude E. (October 1949). "Communication Theory of Secrecy Systems" (https://web.archive.org/web/20120120001953/http://www.alcatel-lucent.com/bstj/vol28-1949/articles/bstj28-4-656.pdf#) (PDF). *Bell System Technical Journal*. **28** (4): 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x (https://doi.org/10.1002%2Fj.1538-7305.1949.tb00928.x). Archived from the original (http://www3.alcatel-lucent.com/bstj/vol28-1949/articles/bstj28-4-656.pdf) (PDF) on 2012-01-20. Retrieved 2011-12-21.
17. Lars R. Knudsen & Matthew Robshaw (2011). *The Block Cipher Companion* (https://books.google.com/?id=YiZKt_FcmYQC&pg=PA11&dq=security+concerns+for+high+quality+cipher#v=onepage&q=security%20concerns%20for%20high%20quality%20cipher&f=false). Springer Science & Business Media. pp. 1–14. ISBN 9783642173424. Retrieved 26 July 2017.
18. Schneier, Bruce. "One-Time Pads" (http://www.schneier.com/crypto-gram-0210.html#7). Archived (https://web.archive.org/web/20050403200231/http://www.schneier.com/crypto-gram-0210.html#7) from the original on 2005-04-03.
19. Singh, Simon (2000). *The Code Book*. United States: Anchor Books. p. 123. ISBN 978-0-385-49532-5.
20. "The Translations and KGB Cryptographic Systems" (https://web.archive.org/web/20090510052927/http://www.nsa.gov/about/_files/cryptologic_heritage/publications/coldwar/venona_story.pdf) (PDF). *The Venona Story*. Fort Meade, Maryland: National Security Agency. 2004-01-15. pp. 26–27 (28–29th of 63 in PDF). Archived from the original (http://www.nsa.gov/about/_files/cryptologic_heritage/publications/coldwar/venona_story.pdf) (PDF) on 2009-05-10. Retrieved 2009-05-03. "...KGB's cryptographic material manufacturing center in the Soviet Union apparently reused some of the pages from one-time pads. This provided Arlington Hall with an opening."

21. Safavi-Naini, Reihaneh (22 July 2008). *Information Theoretic Security: Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings* (https://books.google.com/?id=ySZwUT4nyPsC&lpg=PA223&dq=malleable+one+time+pad&pg=PR1#v=onepage&q=malleable+one+time+pad&f=false). Springer Science & Business Media. ISBN 9783540850922 – via Google Books.
22. A "way to combine multiple block algorithms" so that "a cryptanalyst must break both algorithms" in §15.8 of Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C by Bruce Schneier. Wiley Computer Publishing, John Wiley & Sons, Inc.
23. Introduction to modern cryptography, J Katz, Y Lindell – 2008 – cs.biu.ac.il
24. Kahn, David (1996). *The Codebreakers*. Macmillan. pp. 402–3. ISBN 978-0-684-83130-5.
25. "Stasi Sprach Morse Machine" (https://web.archive.org/web/20150313143905/http://www.numbers-stations.com/sprach-machine). The Numbers Stations Research and Information Center. Archived from the original (http://www.numbers-stations.com/sprach-machine) on March 13, 2015. Retrieved March 1, 2015.
26. Kahn. *The Codebreakers*. p. 715.
27. (http://www.seas.harvard.edu/courses/emr12/4.pdf)*dead link*] http://www.seas.harvard.edu/courses/emr12/4.pdf page 91
28. Jenkin, Tim (May–October 1995). "Talking to Vula: The Story of the Secret Underground Communications Network of Operation Vula" (https://web.archive.org/web/20140826115901/http://www.anc.org.za/show.php?id=4693). *Mayibuye*. Archived from the original (http://www.anc.org.za/show.php?id=4693) on 2014-08-26. Retrieved 24 August 2014. "Our system was based on the one-time pad, though instead of having paper pads the random numbers were on a disk."
29. Pidgeon, Geoffrey (2003). "Chapter 28: Bill Miller – Tea with the Germans". *The Secret Wireless War – The story of MI6 Communications 1939-1945*. UPSO Ltd. p. 249. ISBN 978-1-84375-252-3.
30. Boak, David G. (July 1973) [1966]. *A History of U.S. Communications Security; the David G. Boak Lectures, Vol. I* (https://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NSA_1973u.pdf) (pdf) (2015 declassification review ed.). Ft. George G. Meade, MD: U.S. National Security Agency. Archived (https://web.archive.org/web/20170525181251/http://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NSA_1973u.pdf) (PDF) from the original on 2017-05-25. Retrieved 2017-04-23.
31. Klein, Melville (2003). "Securing Record Communications: The TSEC/KW-26" (https://web.archive.org/web/20060213165531/http://www.nsa.gov/publications/publi00017.pdf) (PDF). NSA. Archived from the original (http://www.nsa.gov/publications/publi00017.pdf) (PDF) on 2006-02-13. Retrieved 2006-05-12.
32. Erskine, Ralph, "Enigma's Security: What the Germans Really Knew", in "Action this Day", edited by Ralph Erskine and Michael Smith, pp 370–386, 2001.
33. "The Venona Translations" (https://web.archive.org/web/20090510052927/http://www.nsa.gov/about/_files/cryptologic_heritage/publications/coldwar/venona_story.pdf) (PDF). *The Venona Story*. Fort Meade, Maryland: National Security Agency. 2004-01-15. p. 17th (of 63 in PDF) but marked 15. Archived from the original (http://www.nsa.gov/about/_files/cryptologic_heritage/publications/coldwar/venona_story.pdf) (PDF) on 2009-05-10. Retrieved 2009-05-03. "Arlington Hall's ability to read the VENONA messages was spotty, being a function of the underlying code, key changes, and the lack of volume. Of the message traffic from the KGB New York office to Moscow, 49 percent of the 1944 messages and 15 percent of the 1943 messages were readable, but this was true of only 1.8 percent of the 1942 messages. For the 1945 KGB Washington office to Moscow messages, only 1.5 percent were readable. About 50 percent of the 1943 GRU-Naval Washington to Moscow/Moscow to Washington messages were read but none from any other year."

Further reading

- Rubina, Frank (1996). "One-Time Pad cryptography". *Cryptologia*. **20** (4): 359–364. doi:10.1080/0161-119691885040 (https://doi.org/10.1080%2F0161-119691885040). ISSN 0161-1194 (https://www.worldcat.org/issn/0161-1194).
- Fostera, Caxton C. (1997). "Drawbacks of the One-time Pad". *Cryptologia*. **21** (4): 350–352. doi:10.1080/0161-119791885986 (https://doi.org/10.1080%2F0161-119791885986). ISSN 0161-1194 (https://www.worldcat.org/issn/0161-1194).

External links

- Detailed description and history of One-time Pad (http://users.telenet.be/d.rijmenants/en/onetimepad.htm) with examples and images on Cipher Machines and Cryptology (http://users.telenet.be/d.rijmenants)
- The FreeS/WAN glossary entry (http://www.freeswan.org/freeswan_trees/freeswan-2.06/doc/glossary.html#OTP) with a discussion of OTP weaknesses