Vernam

The foundation for such a cipher was laid by an American Telephone and Telegraph (AT&T) engineer Gilbert Vernam, who, in 1917, was working in the telegraph section of the company and concentrating on the newest development in telegraphy – the teletype(writer). A few months after World War One broke out, the telegraph section members began investigating the security of the teletype.

The teletype used a code similar to Morse code to transmit messages. The code was named the Baudot code after its French inventor J.M.E. Baudot. The code consisted of 32 combinations of marks and spaces – 26 for the letters of the alphabet and 6 for keyboard commands (like *space, carriage return,* and *shift*). The letters of the alphabet were enciphered as follows (1 = mark and 0 = space):

```
A = 11000 B = 10011 C = 01110 D = 10010 E = 10000
F = 10110 G = 01011 H = 00101 I = 01100 J = 11010
K = 11110 L = 01001 M = 00111 N = 00110 O = 00011
P = 01101 Q = 11101 R = 01010 S = 10100 T = 00001
U = 11100 V = 01111 W = 11001 X = 10111 Y = 10101
Z = 10001
```

Through an electrical arrangement involving rotating commutators, the proper sequence of pulses is sent out when a character's key is struck on the keyboard. … At the receiving end, the incoming pulses energize electromagnets that, in combination, select the proper character and print it. In the punched paper tape which is frequently used to run teletypewriters, marks are represented by holes and spaces by leaving the tape intact. To read the tape, metal fingers push through the holes to make contact and thereby send pulses [this is a 1]; where there is a space, the paper keeps the fingers from completing the circuit [this is a 0].

Vernam suggested punching a tape of key characters and electromechanically adding its pulses to those of the plaintext, the "sum" to constitute the ciphertext. The addition would have to be reversible so that the receiver could subtract the key pulses from the cipher pulses and get the plaintext. Kahn, David, *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*, Scribner, 1996.

Here are the four possible cases and Vernam's rules for addition:

plaintext		key		ciphertext
mark	+	mark	=	space
mark	+	space	=	mark
space	+	mark	=	mark
space	+	space	=	space

Addition modulo 2 is exactly what is needed. Notice that with 1 = mark and 0 = space, Vernam's rules exactly correspond to addition modulo 2.

	0	1
0	0	1
1	1	0

Vernam's rules also exactly corresponds to the operation XOR – exclusive OR. A XOR B means that either statement A is true or statement B is true but not both.

	B is false.	B is true.
A is false.	A XOR B is false.	A XOR B is true.
A is true.	A XOR B is true.	A XOR B is false.

Let us take the word `the` in Baudot code (with 1 and 0 rather than mark and space) 000010010110000 and add to it the random key string 100010000101100

$$\begin{array}{r} 000010010110000 \\ 100010000101100 \\ \hline 100000010011100 \end{array}$$

Notice that (because in addition modulo 2, 0 + 0 = 0 and 1 + 1 = 0) adding the random key string 100010000101100 to the ciphertext 100000010011100 returns plaintext

100000010011100
100010000101100
000010010110000

In addition modulo 2, the additive inverse of 0 is 0 and the additive inverse of 1 is 1. So, the effective of adding the key twice (once to encrypt and once to decrypt) is to do nothing.

100010000101100
100010000101100
000000000000000

Therefore, the same random keystring can be used for encrypting and decrypting.

> To combine the pulses electrically Vernam devised an arrangement of magnets, relays, and bus-bars. Since encipherment and decipherment were reciprocal, the same arrangement served for both. He fed the pulses into this device from two tape readers – one for the keytape, the other for plaintext tape. The mechanism closed a circuit, resulting in a mark, when the two incoming pulses were different, and opened a circuit, resulting in a space when they were the same. The output of marks and spaces could be transmitted just like an ordinary teletypewriter message to the received. Here the Vernam apparatus subtracted out the key pulses, which were supplied by an identical keytape, and recreated the original plaintext pulses. …
>
> Plaintext went in and plaintext came out, while anyone intercepting the message between the two endpoints would pick up nothing but a meaningless sequence of marks and spaces. … The advantage [to Vernam's method] was not the mechanical encipherment and printing of the message. That had been accomplished as far back as the early 1870s by two Frenchmen … . Rather it was the assimilation of encipherment into the overall communication process. Vernam created what came to be called "on-line encipherment"… . He freed a fundamental process in cryptography from the shackles of time and

error. He eliminated the need for a human being – the cipher clerk – from the chain of communication.

…

In the first days of development, the Vernam keys took the form of loops of tape perforated with characters drawn from a hat, giving a random keytext. The engineers … soon spotted the flaw with this. The Vernam system is polyalphabetic. A 32×32 tableau may be set up with the 32 characters of the Baudot alphabet across the top as plaintext and down the side as keys. Because the Baudot alphabet is public information, the composition of the 32 cipher alphabets filling the body of the tableau would be known. Secrecy in the Vernam system thus resides entirely in its keys. Looped keytapes would pass through the Vernam mechanism at regular intervals, permitting a simple Kasiski solution, even though the key recovered would be incoherent. The engineers made the keytapes extremely long to increase the difficulty of such a solution. But then the keytapes became too hard to handle.

… Morehouse surmounted these difficulties by combining two short keytapes of different lengths in a Vernam device as if one were enciphering the other … . If one loop were 1,000 characters long and the other 999, the one-character difference would produced 999,000 combinations before the sequence would repeat. Kahn, David, *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*, Scribner, 1996.

Mauborgne

[Joseph O.] Mauborgne [who was later to become the Army's Chief Signal Officer] recognized that even this system was not immune to cryptanalysis. [From studying the AT&T system, Mauborgne noted that any] repetition of any kind in the keys of cryptograms under analysis imperils them and perhaps dooms them to solution. It does not matter whether the repetitions lie within a single message or among several … . Repetitions in the key could not be permitted. … He therefore welded together the randomness of the key, created, perhaps almost accidentally by Vernam, and the nonrepetition of the key, discovered by the Army Signal School cryptologists, into what is now called the "one-time [pad]." It consists of a random key used once and only once. It provides a new and unpredictable key character for each plaintext character in the whole ensemble of messages ever to be sent by a group of correspondents.

And it is an unbreakable system. Some systems are unbreakable in practice only, because the cryptanalyst can conceive of ways of solving them if he had enough text and time. The one-time [pad] is unbreakable both in theory and practice. No matter how much text a cryptanalyst had available in it, or how much time he had to work on it, he could never solve it. … Kahn, David, *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*, Scribner, 1996.