Secure Digital Communications

CODES

For purposes of this presentation, I will use the definition of Code as being a mechanism for the purpose of either converting the communication of information from one transmission medium to another or for preserving that information.

Thus the alphabet may be considered to be a code – it is used to convert between aural content and visible content. Prior to audio recording it was the only way to preserve and/or distribute.

CIPHERS

A CIPHER (or CYPHER) is an overlay upon code used to hide or obfuscate the meaning of the communication.

Topics

CODES

Morse **Baudot** **Hollerith** **ASCII**

CIPHERS and ENCRYPTION

Symmetric Key Ciphers

Caesar Cipher
Pre-Shared Key Cipher (PSK)
One-Time Pad

Symbolic Cipher
The Enigma Machine

Asymmetric Key Ciphers

Public Key Encryption (PKE)

AUTHENTICATION

Certificates and Certificate Authorities (CA)
Secure Socket Layer (SSL) and HTTPS

USAGE EXAMPLES

Virtual Private Networks (VPN)
Secure Proxy Services

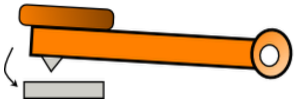
CODE

The use of a code does not of itself imply that it is being used for secrecy or security purposes.

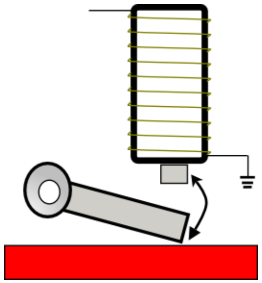
For example the “Morse Code” which converts letters and numbers to sequences of just dots and dashes because the circuitry of a telegraph system with only two states - ON or OFF. This doesn’t lend itself to an analog mechanism (various voltage levels) needed to support the roughly four dozen discrete values to represent the alphabet, and 10 digits and a few symbols.

Morse Code

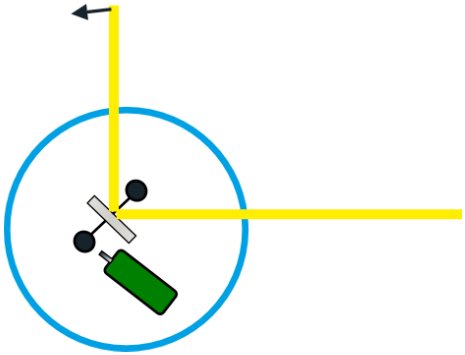
Samuel Mores (1791-1872) demonstrated his one-wire telegraph system to Congress in 1844 with a message sent from Baltimore to Washington.



KEY



Sounder



Trans-Atlantic Receiver - 1858

International Morse Code

1. The length of a dot is one unit.
2. A dash is three units.
3. The space between parts of the same letter is one unit.
4. The space between letters is three units.
5. The space between words is seven units.

A	● ▬
B	▬ ● ● ●
C	▬ ● ▬ ●
D	▬ ● ●
E	●
F	● ● ▬ ●
G	▬ ▬ ●
H	● ● ● ●
I	● ●
J	● ▬ ▬ ▬
K	▬ ● ▬
L	● ▬ ● ●
M	▬ ▬
N	▬ ●
O	▬ ▬ ▬
P	● ▬ ▬ ●
Q	▬ ▬ ● ▬
R	● ▬ ●
S	● ● ●
T	▬

U	● ● ▬
V	● ● ● ▬
W	● ▬ ▬
X	▬ ● ● ▬
Y	▬ ● ▬ ▬
Z	▬ ▬ ● ●

1	● ▬ ▬ ▬ ▬
2	● ● ▬ ▬ ▬
3	● ● ● ▬ ▬
4	● ● ● ● ▬
5	● ● ● ● ●
6	▬ ● ● ● ●
7	▬ ▬ ● ● ●
8	▬ ▬ ▬ ● ●
9	▬ ▬ ▬ ▬ ●
0	▬ ▬ ▬ ▬ ▬

Baudot Code

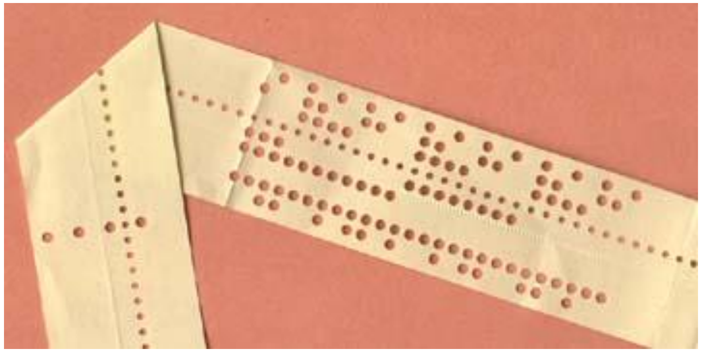
Predecessor of the ASCII code in common use today was BAUDOT (by Emile Baudot 1845 - 1903) who developed a code that would let machines send data via a wired connection. It evolved into the code used by Teletypes etc. Unlike the Morse code where the character was identified by the duration of the electric pulses and pauses, and characters were separated by a longer ‘silent’ period, all Baudot characters required the same duration as each required the same total number of time ticks whether a tick was ON or OFF.

The unit of measure for the transmission of one character was the ‘baud’.

It error correction was included for each character, 10 timer ticks were required per character. Thus 300 baud supported 30 cps.

Machine-Readable

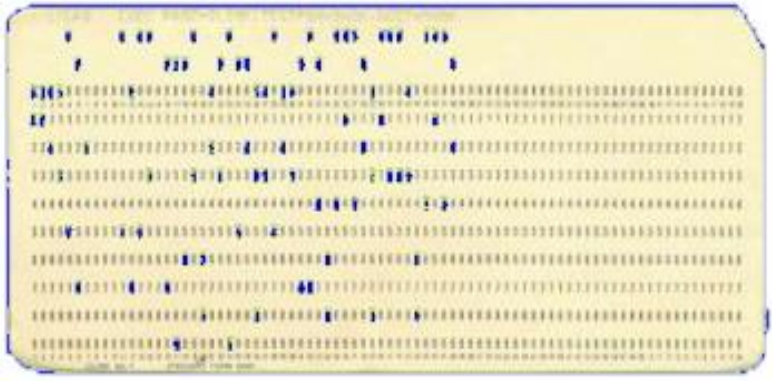
Eventually the message could be prepared via punching holes in a paper tape and then transmitted and received at a constant speed. Upon reception it could be printed directly, or punched to tape and later played back and printed.



A similar system was used for the ‘ticker tape’ for reporting stock prices and transactions.

Typical Teletype machine ran at 100 baud, or 10cps.

Hollerith



Punch cards were used to control various manufacturing processes such as weaving, even carnival organs, but in 1890 Herman Hollerith (1860-1929) used them to store machine-readable data for the 1890 census. It evolved into the ubiquitous “IBM card” which had 80 columns, each with 12 punch positions.

A single punch in one of the lower 10 rows denoted a digit.

The top two rows were called “Zone” rows and were provided for multiple punches in the same column. Thus alphabetic or special characters such as period, comma, currency etc. were supported.

The keypunch machine could also print above the top row.

ASCII CODE

0 NUL	32	64 @	96 `
1 SOH Start of Header	33 !	65 A	97 a
2 STX Start of Text	34 "	66 B	98 b
3 ETX End of Text	35 #	67 C	99 c
4 EOT End of Transmission	36 $	68 D	100 d
5 ENQ Enquiry	37 %	69 E	101 e
6 ACK Aknowledge	38 &	70 F	102 f
7 BEL Bell	39 '	71 G	103 g
8 BS Backspace	40 (	72 H	104 h
9 TAB Tab	41)	73 I	105 i
10 LF Line Feed	42 *	74 J	106 j
11 VT Vertical Tab	43 +	75 K	107 k
12 FF Form Feed	44 ,	76 L	108 l
13 CR Carriage Return	45 -	77 M	109 m
14 SO Shift Out	46 .	78 N	110 n
15 SI Shift In	47 /	79 O	111 o
16 DLE Data Link Escape	48 0	80 P	112 p
17 DC1 Device Control 1	49 1	81 Q	113 q
18 DC2 Device Control 2	50 2	82 R	114 r
19 DC3 Device Control 3	51 3	83 S	115 s
20 DC4 Device Control 4	52 4	84 T	116 t
21 NAK Negative Acknowledgement	53 5	85 U	117 u
22 SYN Synchronous Idle	54 6	86 V	118 v
23 ETB End of Transmission Block	55 7	87 W	119 w
24 CAN Cancel	56 8	88 X	120 x
25 EM End of Medium	57 9	89 Y	121 y
26 SUB Substitute	58 :	90 Z	122 z
27 ESC Escape	59 ;	91 [	123 {
28 FS Field Separator	60 <	92 \	124 |
29 GS Group Separator	61 =	93]	125 }
30 RS Record Separator	62 >	94 ^	126 ~
31 US Unit Separator	63 ?	95 _	127 DEL

American Standard Code for Information Interchange

Sending a character via an asynchronous connection example:

Uppercase Y is coded as 89.
In binary that is 1011001.
(64+16+8+1)
Start bit = 1
7 Data bits: 1011001
Parity bit: 1 (assuming ODD parity)
Stop bit: 1
10 bits total.

At 300 baud get 30 cps

Ciphers / Encryption

So far we have been using codes as a mechanism for transmitting data from point A to point(s) B. We have not been concerned with secrecy, our goal has been just to get the information moved.

We will now examine ways to manipulate the message so that casual or unauthorized viewers can not easily determine its content. This is done by using a cipher (or cypher). Application of the process is called encryption.

Symmetric Key Ciphers

A symmetric key cipher makes use of the same key for encrypting and decrypting the data. It is good for such things as protecting data on disks and/or sharing data within a closed community, but not good for sending a secure message to someone outside of the community as it would require distributing the key, and that distribution would in itself have to be done in a secure (i.e. alternate channel) process.

Symmetric Key Ciphers

Examples of symmetric ciphers are DES, Blowfish, Twofish, Threefish, AES, etc., as well as a layer within PGP.

In general symmetric ciphers are fast and hard to break. They tend to be mathematically complex.

The examples that follow are simplistic but illustrate several types of symmetric ciphers.

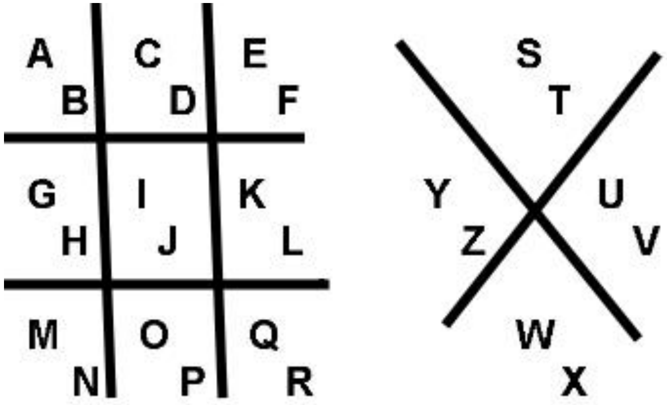
Caesar Cipher

Named after Julius Caesar who used it for personal communications, however he surely did not originate it. A Caesar Cipher is a straight forward substitution cipher where each letter is replaced by a substitute usually based upon a simple shift within the alphabet. In the following example, the shift is 5.

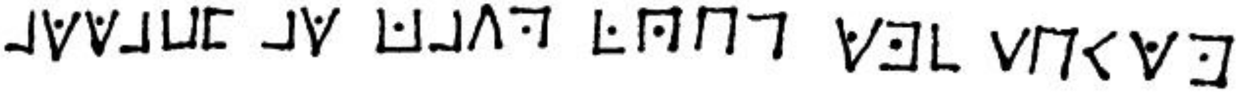
Plain:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
CIPHER:	FGHIJKLMNOPQRSTUVWXYZABCDE
Text:	ATTACK AT DAWN FROM THE SOUTH
Encrypted:	FYYFHPEFYEIFASEKWTREYMJEXTZYM

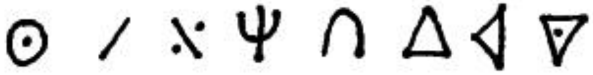
This is an easy cipher to crack. For example, if the encrypted text is fairly long, a statistical analysis of letter frequency can be compared against the frequency distribution of letters in the language. Back in the 1840s Morse built his code using E and T as the most common, followed by M, N, A and I etc.

SYMBOLIC CIPHER



Here's a cipher my grandfather showed me many years ago. Convert the letter to a symbol consisting of the lines in the grid adjacent to the letter you want. If it is the second letter add a dot inside the lines.

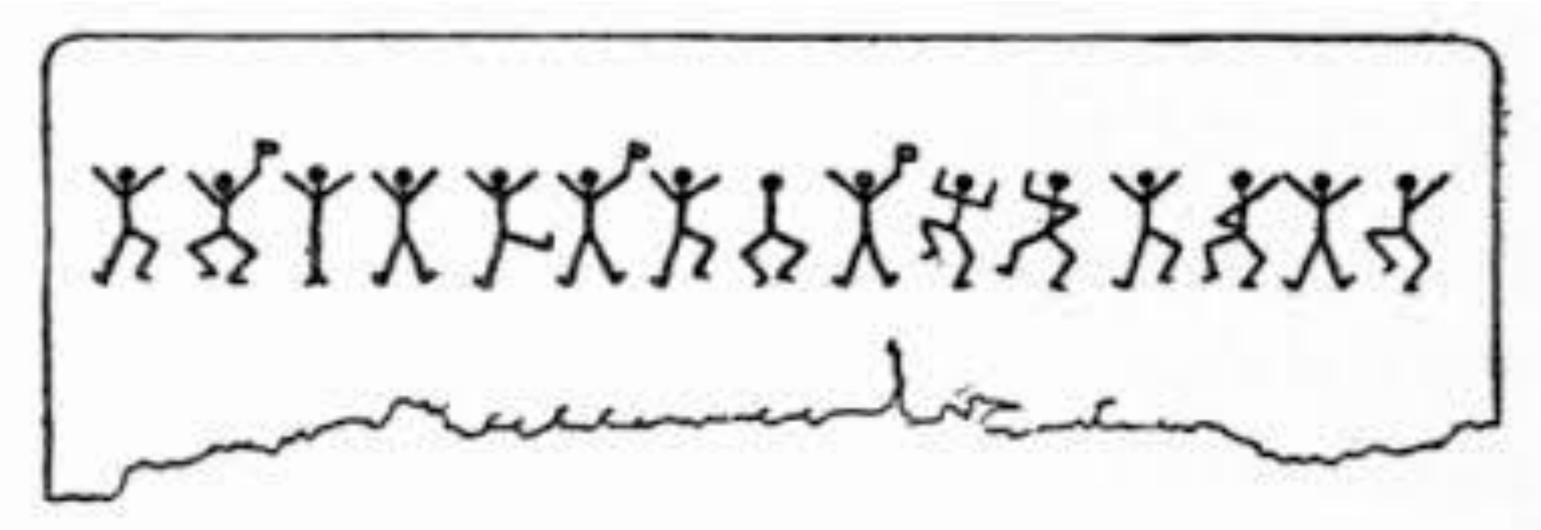




If you are feeling paranoid liberally intersperse some 'noise' symbols, such as shown in the second line.

SYMBOLIC CIPHER

A symbol substitution cipher was central to the plot of a Sherlock Holmes short story "The Adventure of the Dancing Men" c. 1890.



PRE-SHARED KEY (PSK)

By use of a key string rather than a single shift, a more complex substitution may be applied. To do this, the recipient must know the key string.

```
Plain:        ABCDEFGHIJKLMNOPQRSTUVWXYZ
PSK-KEY:      CUMBERLANDCUMBERLANDCUMBER

Text:         ATTACK AT DAWN FROM THE SOUTH
Encrypted:    DNFCHBLBGDGVIPEXCP DWBRBXFFUV
```

Notice that in this case the two “A”s at the start come out with different letters since the first A is shifted by the index position of C (3) and the second by the index position of B (2). In the same way the first T is shifted by the index position of U and the second by the index position of M. This results in a harder cipher to crack, but by use of a computer that generates and tests relatively short keywords it is still not a very secure mechanism. In this example the PSK is only 10 characters long. In this method the longest key may only be 26 characters long as a character may not be repeated.

The ENIGMA MACHINE

Consider three rotors each of which have 26 different substitutions. Let’s say the electrical signals travels right to left through the three adjacent rotors.

Add a “reflector” which adds one substitution and then sends the signal back through the same three rotors left to right for a total of 7 substitutions.

Every time a character is processed the first rotor is stepped by one, until it has stepped 26 times, at which point the next rotor is stepped. This is much like the odometer on an automobile.

When the second rotor is stepped 26 times the third rotor is stepped, and after the 3rd rotor steps 26 times things repeat.

In this way, the substitution key is not repeated until 26 *cubed (17,576)* characters have been sent.

The ENIGMA MACHINE

To further complicate things, there are 6 combinations of ways that the rotors may be put into the machine:

1 2 3	**1 3 2**
2 1 3	**2 3 1**
3 1 2	**3 2 1**

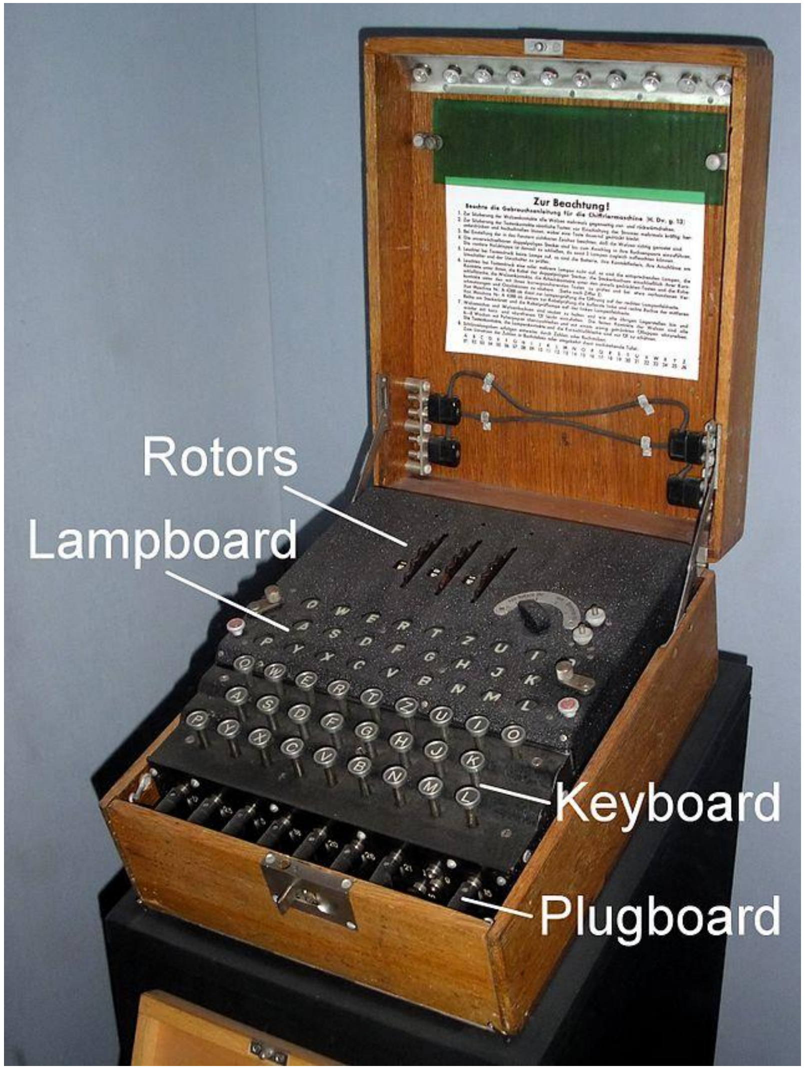
and further you may start with each rotor at a different position. Thus there are 6 x 26 x 26 x 26 possible *starting* keys, each 26 cubed in length.

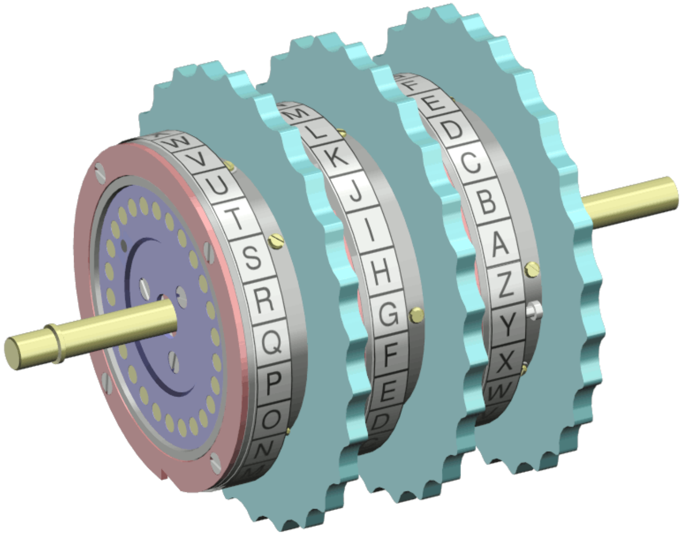
Thus the key for a particular day might be this starting setting:
Left : 2 at “F” Middle: 1 at “X” Right: 3 at “P”

This was the German Enigma machine used extensively during World War II. It was about the size of a typewriter but instead of printing, pressing a key turned on a light - one for each character. The pre-shared key consisted of the rotor sequence and the initial position of each and changed every day.

It was thought to be unbreakable.

Enigma Machine





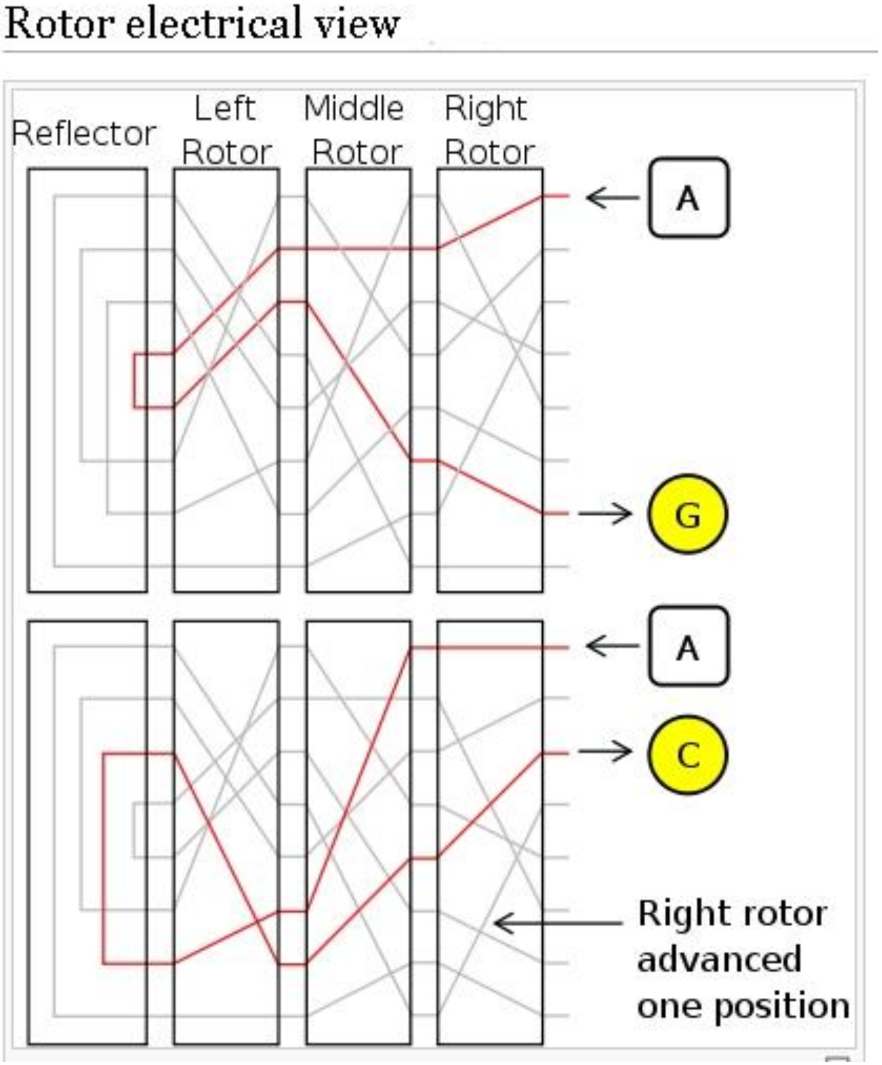
The ENIGMA MACHINE

It was thought to be unbreakable.

It wasn’t. Before the war, the Polish intelligence service had captured a machine and smuggled it to England just before Poland was invaded. The British built an electro-mechanical computer that replicated the operation and was able to decrypt their traffic. Information gained from this system was known as ULTRA.

The analysts still had to determine the rotor settings for the day, but once that was done they could read the German transmissions. Later in the war a submarine was captured, boarded, and the top-secret book of rotor settings for the German Navy was retrieved.

The ENIGMA MACHINE

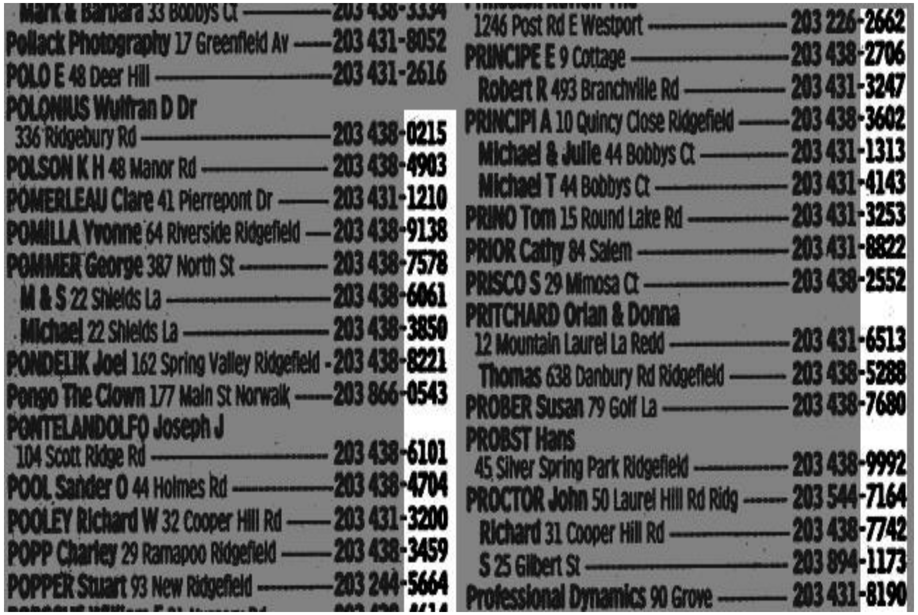


ONE-TIME PAD

This requires an identical source of a sequence of random numbers to be available to both correspondents. I think I remember that in the 50's a Russian spy in NYC used the Brooklyn white pages as his number sequence source. Based upon the date and the sequence number of the message if more than one message was to be encoded, a calculation would be made to select a page, column and line upon the page. He would start with that item and make use of each of the last four digits of the phone numbers in the list. The individual digits were then used to determine the offset for a substitution index.

ONE-TIME PAD

	ABCDEFGHIJKLMNOPQRSTUVWXYZ
0	ABCDEFGHIJKLMNOPQRSTUVWXYZ
1	BCDEFGHIJKLMNOPQRSTUVWXYZA
2	CDEFGHIJKLMNOPQRSTUVWXYZAB
3	DEFGHIJKLMNOPQRSTUVWXYZABC
4	EFGHIJKLMNOPQRSTUVWXYZABCD
5	FGHIJKLMNOPQRSTUVWXYZABCDE
6	GHIJKLMNOPQRSTUVWXYZABCDEF
7	HIJKLMNOPQRSTUVWXYZABCDEFG
8	IJKLMNOPQRSTUVWXYZABCDEFGH
9	JKLMNOPQRSTUVWXYZABCDEFGHI



Mark & Barbara 33 Bobbys Ct	203 438-3334
Pollack Photography 17 Greenfield Av	203 431-8052
POLO E 48 Deer Hill	203 431-2616
POLONIUS Wulfran D Dr	
336 Ridgebury Rd	203 438-0215
POLSON K H 48 Manor Rd	203 438-4903
POMERLEAU Clare 41 Pierrepont Dr	203 431-1210
POMILLA Yvonne 64 Riverside Ridgefield	203 438-9138
POMMER George 387 North St	203 438-7578
M & S 22 Shields La	203 438-6061
Michael 22 Shields La	203 438-3850
PONDELIK Joel 162 Spring Valley Ridgefield	203 438-8221
Pongo The Clown 177 Main St Norwalk	203 866-0543
PONTELANDOLFO Joseph J	
104 Scott Ridge Rd	203 438-6101
POOL Sander O 44 Holmes Rd	203 438-4704
POOLEY Richard W 32 Cooper Hill Rd	203 431-3200
POPP Charley 29 Ramapoo Ridgefield	203 438-3459
POPPER Stuart 93 New Ridgefield	203 244-5664
1246 Post Rd E Westport	203 226-2662
PRINCIPE E 9 Cottage	203 438-2706
Robert R 493 Branchville Rd	203 431-3247
PRINCIPI A 10 Quincy Close Ridgefield	203 438-3602
Michael & Julie 44 Bobbys Ct	203 431-1313
Michael T 44 Bobbys Ct	203 431-4143
PRINO Tom 15 Round Lake Rd	203 431-3253
PRIOR Cathy 84 Salem	203 431-8822
PRISCO S 29 Mimosa Ct	203 438-2552
PRITCHARD Orlan & Donna	
12 Mountain Laurel La Redd	203 431-6513
Thomas 638 Danbury Rd Ridgefield	203 438-5288
PROBER Susan 79 Golf La	203 438-7680
PROBST Hans	
45 Silver Spring Park Ridgefield	203 438-9992
PROCTOR John 50 Laurel Hill Rd Ridg	203 544-7164
Richard 31 Cooper Hill Rd	203 438-7742
S 25 Gilbert St	203 894-1173
Professional Dynamics 90 Grove	203 431-8190

The sequence was used only once, hence the name “One-Time Pad”. If the number sequence is truly random and the sequence is never repeated (i.e. ‘looped’) within the same message or other messages, the One-Time Pad is considered to be unbreakable. However for practical reasons it is seldom used.

Symmetric Key Ciphers

A symmetric key cipher makes use of the same key for encrypting and decrypting the data. It is good for such things as protecting data on disks and/or sharing data within a closed community, but not good for sending a secure message to someone outside of the community as it would require distributing the key, and that distribution would in itself have to be done in a secure (i.e. alternate channel) process.

Symmetric Key Ciphers

Examples of symmetric ciphers are DES, Blowfish, Twofish, Threefish, AES, etc., as well as a layer within PGP.

In general symmetric ciphers are fast and hard to break. They tend to be mathematically complex.

Symmetric Example – Wi-Fi

When you establish a secure Wi-Fi connection, you must know the “Pass Phrase” which is actually the Pre-Stored Key for the connection. This gives you a fairly secure connection between your device (computer, tablet, smartphone, etc.) and the Wi-Fi access point, which is usually built into the router. The Wi-Fi encryption is stripped within the Access Point.

Note that the data packet itself may be encrypted via another mechanism such as SSL for transmission through the Internet.

Asymmetric Key Ciphers

An Asymmetric Key Cipher makes use of two keys – one to encrypt and one to decrypt. Asymmetric ciphers are typically used where a communications link might be monitored and thus must be secured. Thus it is wrapped around the data transmission, but not the ‘addressing envelope” such as the source and destination IP address etc.

It is not used for storage media (i.e. the disk system at the server.)

The example that follows is a generic description of PKE – Public Key Encryption as used by Secure Socket Layer – the most commonly used mechanism for web browser to remote server session security.

Asymmetric Key Encryption

Asymmetric Key encryption utilizes two distinct and complementary keys – one to encode, and the other to decode.

PUBLIC KEY ENCRPTION (PKE)

The current state-of-the-art encryption mechanism *in general use by individuals and corporations* for digital communications is Public Key Encryption. It uses asymmetric keys.

The keys are known as a PRIVATE key, known only to the sender, and a PUBLIC key that is distributed to anyone to whom he/she wishes to bi-directionally exchange secure messages.

The key pair is generated by the use of two very large prime numbers.

Public Key Encryption (PKE)

The PUBLIC key can decrypt a message encrypted by the PRIVATE key. Conversely a message encrypted by the PUBLIC key can be decrypted by the PRIVATE key.

A message encrypted by one of these keys CAN NOT be decrypted by that same key!

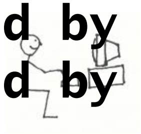
PUBLIC KEY ENCRPTION (PKE)

Key Owner

Correspondent

```
Encrypted by PRIVATE key,
decrypted by PUBLIC key ->

<- Encrypted by PUBLIC key,
   decrypted by PRIVATE key
```

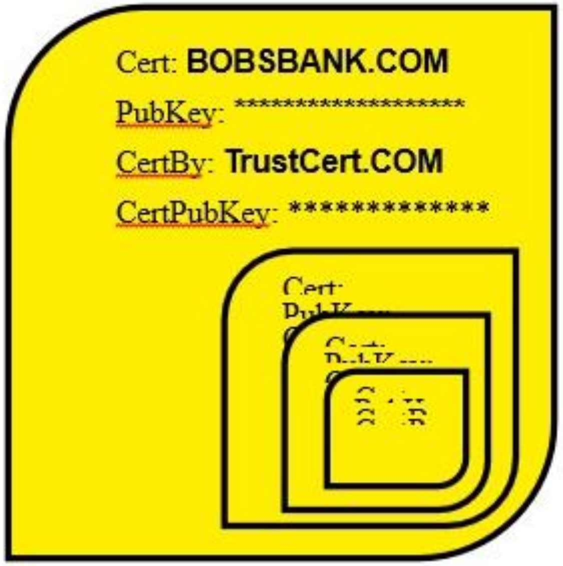


To "digitally sign" a document, the Correspondent (on the right in the above) would use *his* PRIVATE key and the document recipient (on the left) would use the PUBLIC key of the sender (signer) to authenticate the sender's digital signature.

AUTHENTICATION

For PKE to work, it is necessary for the sender’s PUBLIC key to be available to the recipient. The recipient must also have a way to determine that the key really belongs to the sender, i.e. that it is *authentic*. This is done via a digital certificate mechanism.

DIGITAL CERTIFICATE



Cert: BOBSBANK.COM

PubKey: *******************

CertBy: TrustCert.COM

CertPubKey: *************

A digital certificate contains the Public Key for a site, as well as nested *and encrypted* digital certificates which are used to authenticate the enclosing certificate.

AUTHENTICATION

Let’s say that you want to establish a secure connection with BOBSBANK.COM using your web browser.

When you go to a page requiring security (HTTPS) you get a page which provides a digital certificate which must be authenticated before the page is displayed. This certificate contains the PUBLIC key for the page, or more likely, the BOBSBANK.COM domain. The certificate also contains an *encrypted* certificate created by a company that certifies that BOBSBANK is who they say they are. But who vouches for them? The answer is that *their* encrypted certificate contains an encrypted certificate by who ever vouches for them. This continues in a nest until you finally get to a CERTIFICATE AUTHORITY (a.k.a. “CA”) The CA’s certificate does NOT contain their PUBLIC key.

AUTHENTICATION

So how do you authenticate the CA's certificate?

The answer is that your computer contains a "digital key ring" originally loaded by your operating system's installation. It has the PUBLIC keys for the common 'root' CAs.

VeriSign *(now part of Symantec, as are Thawte and Geotrust)*

Comodo Group GoDaddy GlobalSIgn

Some governments provide CA services. An enterprise may also generate a digital certificate itself for internal use, i.e. within its own domain. To do that it must then put its Public Key on the key ring of its client machines.

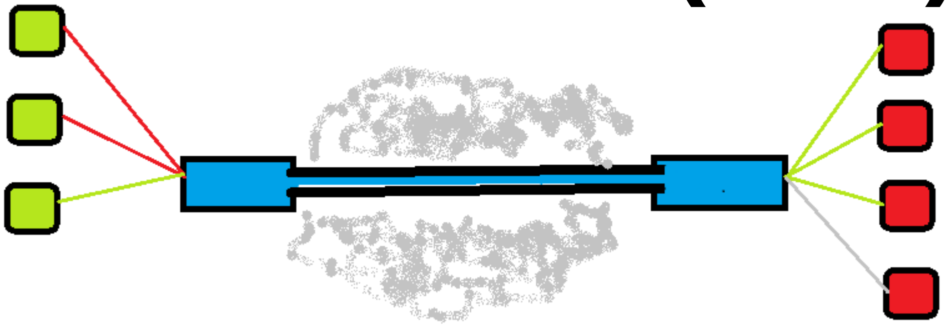
There is a mechanism for Digital Certificate revocation.

SECURE SOCKET LAYER (SSL)

Once you have authenticated the certificate for your correspondent, you establish a secure socket layer in your communications protocol stack. The data content of your communications is processed using the PUBLIC key when you receive or send. You typically start by sending your encrypted logon credentials.

The recipient (*BOBSBANK in our example*) uses the PRIVATE key to decrypt. BOBSBANK encrypts data sent to you using the PRIVATE key, and you decrypt it using the PUBLIC key.

VIRTUAL PRIVATE NETWORK (VPN)



Browser to Server is not the only situation where secure communication might be used.

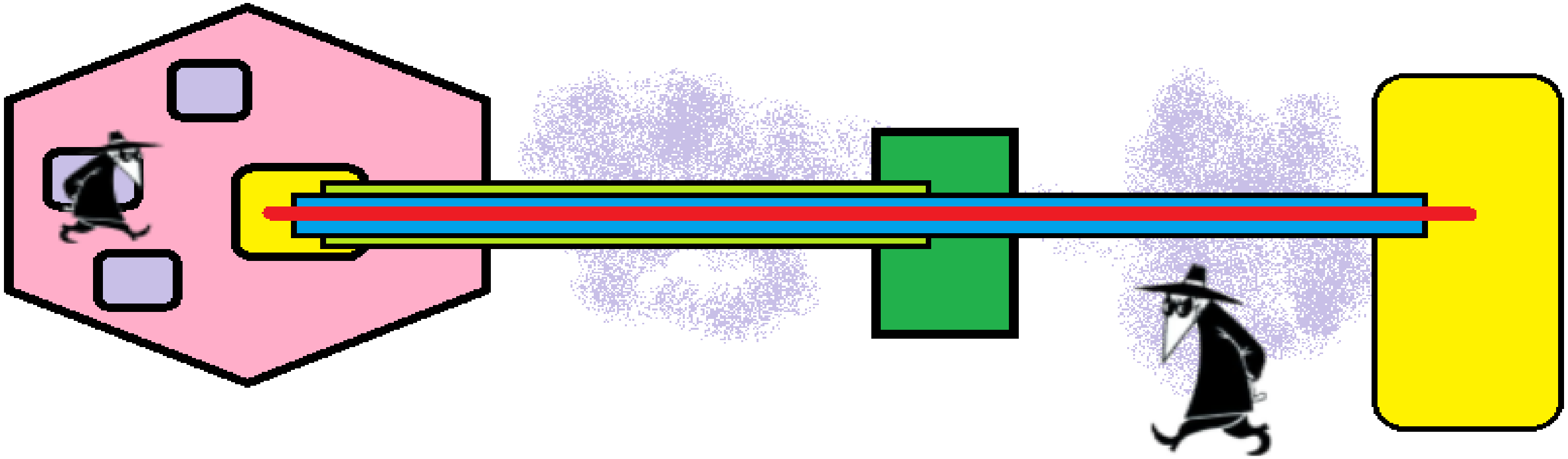
For example, two or more local area networks (LANs) might be connected via a Virtual Private Network. In this illustration two LANs (green machines and red machines) are connected by using a pair of “end-point VPN routers.” They connect the two LANs with a “tunnel” that goes through the Internet such that all traffic (other than the routing information) is encrypted. The encryption/decryption is performed by firmware within the routers.

Each router has the address(es) of other router(s) in the VPN as well as the associated Pre-Shared Key(s).

VIRTUAL PRIVATE NETWORK (VPN)

The previous example used end-point routers. A VPN may also be created using a “client” program on an individual computer so that a portable machine such as a notebook, tablet, or smartphone may establish a VPN tunnel into a site. The site’s end may be managed by an end-point router, or by a VPN service on a machine such as a web or application server.

SECURE PROXY SERVER



Suppose you are using a WiFi network such as a Starbucks, an Internet café, a library or hotel. Typically these are “Open Wi-Fi” (i.e. unsecured) connections. While you might not require an SSL connection for your e-mail, YouTube or Facebook etc., you may still desire privacy or anonymity. To do this you might use a public secure proxy server.

You establish an SSL tunnel to the secure proxy server, thus protecting your WiFi connection. Beyond the proxy server the connection may or may not be encrypted depending upon what is available or required by the remote site.