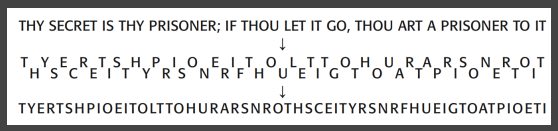
Steganography

1. Secret communication achieved by hiding the existence of a message is known as steganography
2. Shaved head - wrote msg - grow hair
3. ancient Chinese wrote messages on fine silk, which was scrunched into a tiny ball and covered in wax. The messenger would then swallow the ball of wax
4. “milk” of the tithymalus plant could be used as an invisible ink. Although the ink is transparent after drying, gentle heating chars it and turns it brown. Many organic fluids behave in a similar way, because they are rich in carbon and therefore char easily, modern spies who have run out of standard-issue invisible ink to improvise by using their own urine

Cryptography

1. The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning, a process known as encryption.
2. The advantage of cryptography is that if the enemy intercepts an encrypted message, the message is unreadable.
3. Cryptography itself can be divided into two branches, known as transposition and substitution. In transposition, the letters of the message are simply rearranged, effectively generating an anagram
4. Rail fence transposition - which the message is written with alternating letters on separate upper and lower lines. The sequence of letters on the lower line is then tagged on at the end of the sequence on the upper line to create the final encrypted message



5. Spartan scytale transposition - first-ever military cryptographic device, The scytale is a wooden staff around which a strip of leather or parchment is wound, The sender writes the message along the length of the scytale and then unwinds the strip, which now appears to carry a list of meaningless letters. The message has been scrambled. The messenger would take the leather strip, and, as a steganographic twist, he would sometimes disguise it as a belt with the letters hidden on the inside. To recover the message, the receiver simply wraps the leather strip around a scytale of the same diameter as the one used by the sender

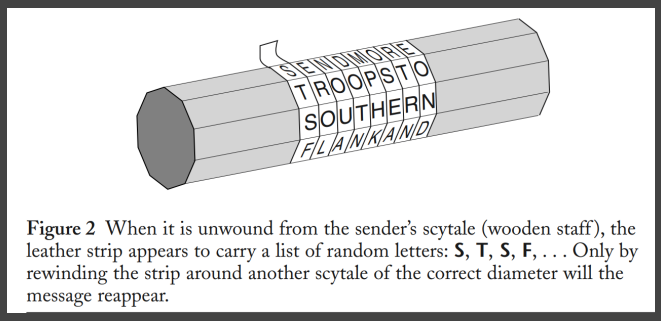


Figure 2 When it is unwound from the sender’s scytale (wooden staff), the leather strip appears to carry a list of random letters: **S**, **T**, **S**, **F**, . . . Only by rewinding the strip around another scytale of the correct diameter will the message reappear.

6. Substitution cipher - each letter in the plaintext (the message before encryption) is substituted for a different letter to produce the ciphertext (the message after encryption)

A	D	H	I	K	M	O	R	S	U	W	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
V	X	B	G	J	C	Q	L	N	E	F	P	T

CUUZ VZ CGXSGIBZ - MEET AT MIDNIGHT

7. Caesar cipher - each letter in the plain alphabet with a letter from a cipher alphabet, and the cipher alphabet is allowed to consist of any rearrangement of the plain alphabet

Plain alphabet	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
Cipher alphabet	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Plaintext	i came, i saw, i conquered
Ciphertext	L FDPH, L VDZ, L FRQTXHUHG

8. Monoalphabetic substitution cipher - in which the cipher alphabet consists of letters, symbols or a mix of both. Eg : a in the plain alphabet might be replaced by # in the cipher alphabet, b might be replaced by +.
9. frequency analysis - reveal the contents of a scrambled message simply by analyzing the frequency of the characters in the ciphertext. (difficult for small words)

Letter	Percentage	Letter	Percentage
a	8.2	n	6.7
b	1.5	o	7.5
c	2.8	p	1.9
d	4.3	q	0.1
e	12.7	r	6.0
f	2.2	s	6.3
g	2.0	t	9.1
h	6.1	u	2.8
i	7.0	v	1.0
j	0.2	w	2.4
k	0.8	x	0.2
l	4.0	y	2.0
m	2.4	z	0.1

10. Code - very specific meaning, and applies only to a certain form of substitution, each word is represented by another word or symbol

assassinate	= D	general	= Σ	immediately	= 08
blackmail	= P	king	= Ω	today	= 73
capture	= J	minister	= Ψ	tonight	= 28

11. Beale Ciphers : Treasure

1 = f	11 = s	21 = b
2 = e	12 = w	22 = n
3 = i	13 = t	23 = l
4 = t	14 = b	24 = e
5 = s	15 = t	25 = n
6 = a	16 = k	26 = p

7 = r	17 = t	27 = t
8 = a	18 = e	28 = b
9 = t	19 = w	29 = f
10 = t	20 = w	30 = e

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975, 14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485, 604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370, 11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500, 538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283, 118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21, 24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131, 160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62, 116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568, 614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4, 30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461, 44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216, 728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5, 81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86, 36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985, 233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62, 194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895, 10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62, 31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31, 86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216, 548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56, 216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617, 84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18, 212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88, 612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132, 40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936, 447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216, 814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84, 221, 736, 820, 214, 11, 60, 760.

I have deposited in the county of Bedford, about four miles from Buford's, in an excavation or vault, six feet below the surface of the ground, the following articles, belonging jointly to the parties whose names are given in number "3," herewith:

The first deposit consisted of one thousand and fourteen pounds of gold, and three thousand eight hundred and twelve pounds of silver, deposited November, 1819. The second was made December, 1821, and consisted of nineteen hundred and seven pounds of gold, and twelve hundred and eighty-eight pounds of silver; also jewels, obtained in St. Louis in exchange for silver to save transportation, and valued at $13,000.

The above is securely packed in iron pots, with iron covers. The vault is roughly lined with stone, and the vessels rest on solid stone, and are covered with others. Paper number "1" describes the exact locality of the vault, so that no difficulty will be had in finding it.

12. Enigma Machine/ Scherbius' design of the Enigma

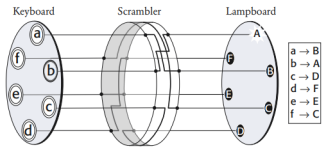


Figure 26 A simplified version of the Enigma machine with an alphabet of just six letters. The most important element of the machine is the scrambler. By typing in **b** on the keyboard, a current passes into the scrambler, follows the path of the internal wiring, and then emerges so as to illuminate the **A** lamp. In short, **b** is encrypted as **A**. The box to the right indicates how each of the six letters is encrypted.

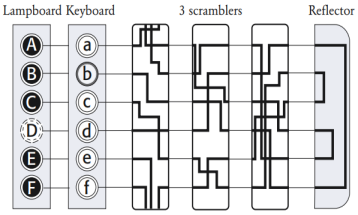


Figure 29 Scherbius' design of the Enigma included a third scrambler and a reflector that sends the current back through the scramblers. In this particular setting, typing in **b** eventually illuminates **D** on the lampboard, shown here adjacent to the keyboard.

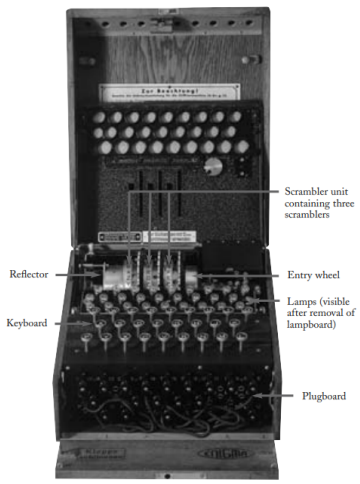


Figure 33 An Enigma machine with the inner lid opened, revealing the three scramblers.

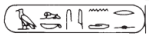
Terminology : encipher means to scramble a message using a cipher, while encode means to scramble a message using a code. Similarly, the term decipher applies to unscrambling an enciphered message, and decode to unscrambling an encoded message. The terms encrypt and decrypt are more general, and cover scrambling and unscrambling with respect to both codes and ciphers

The first stage in Babbage's cryptanalysis is to look for sequences of letters that appear more than once in the ciphertext.

Champollion continued to astonish his peers, mastering Latin, Greek, Hebrew, Ethiopic, Sanskrit, Zend, Pahlavi, Arabic, Syrian, Chaldean, Persian and Chinese, all in order to arm himself for an assault on hieroglyphs.

Table 9 Young's decipherment of  , the cartouche of Ptolemaios (standard version) from the Rosetta stone.

Hieroglyph	Young's sound value	Actual sound value
	p	**p**
	t	**t**
	optional	**o**
	**lo** or **ole**	**l**
	ma or **m**	**m**
	**i**	**i** or **y**
	osh or **os**	**s**

Table 12 Champollion's decipherment of  , the cartouche of Alksentrs (Alexander).

Hieroglyph	Sound value
	**a**
	**l**
	?
	s
	e
	?
	t
	r
	?

Modular arithmetic, sometimes called clock arithmetic in schools, is an area of mathematics that is rich in one-way functions. It deals with a finite group of numbers arranged in a THE CODE BOOK 198 loop, rather like the numbers on a clock.