A Glimpse of the History of Cryptography

Cunsheng Ding
Department of Computer Science
HKUST, Hong Kong, CHINA

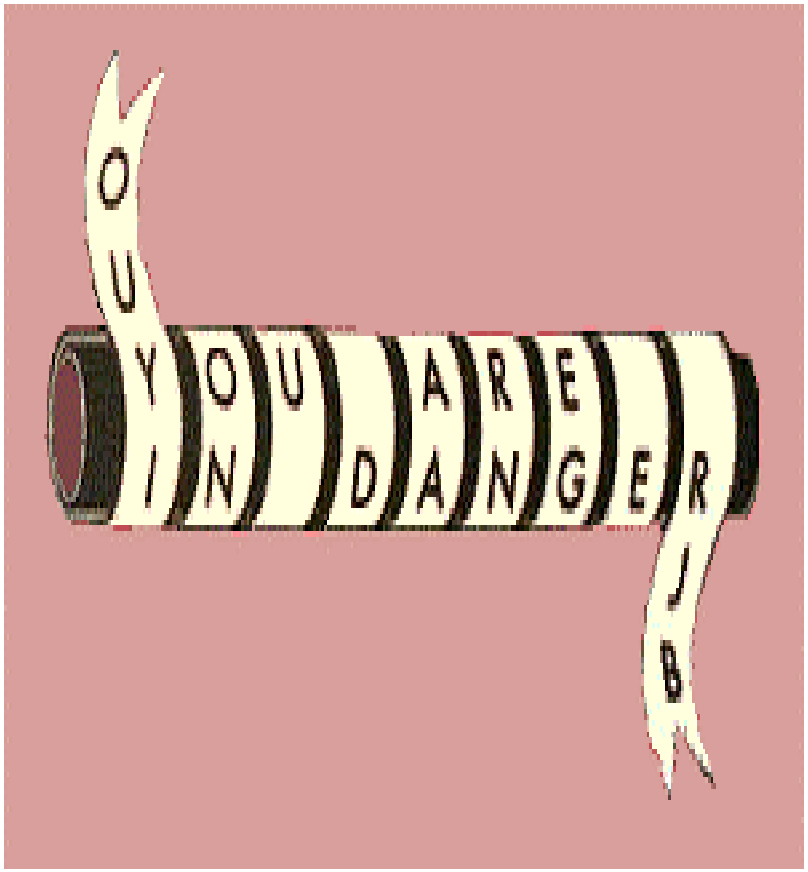
Part I: Manual Ciphers

When Codes Were Used

- Codes and ciphers are methods for encrypting data and messages.
- Codes and ciphers have been used since ancient times (c. 1900 B.C.)
- The word CRYPTOGRAPHY, meaning the science of codes, comes from the Greek words kryptos (secret) and graphos (writing).

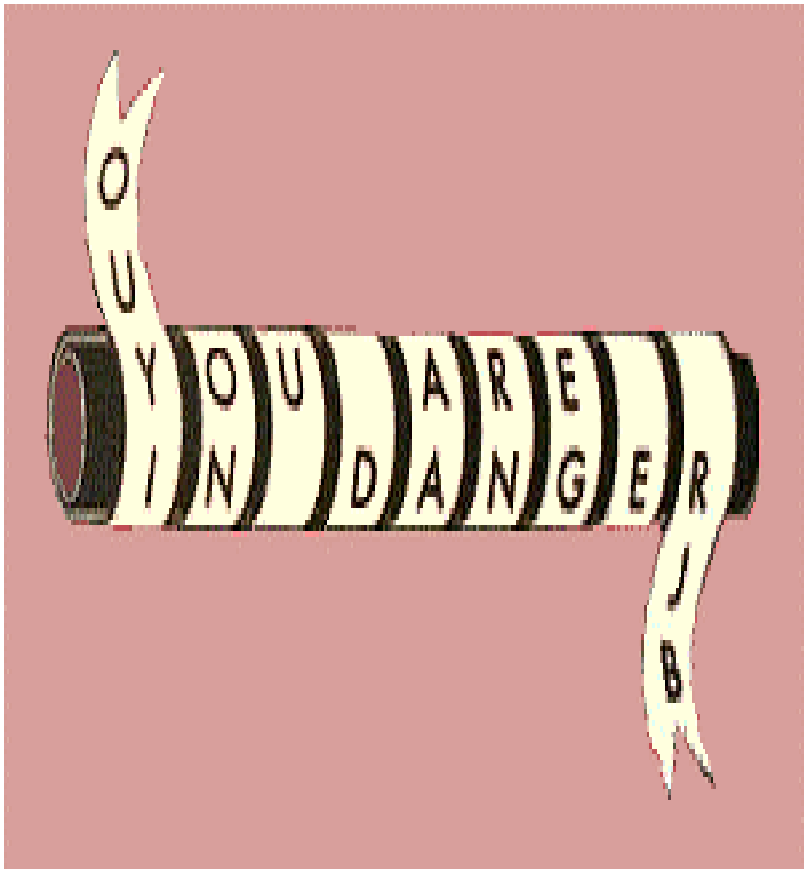
Historical Example 1

- In 405 BC the Greek general LYSANDER OF SPARTA was sent a coded message written on the inside of a servant's belt.



Historical Example 1

- When Lysander wound the belt around a wooden baton the message was revealed. The message warned Lysander that Persia was about to go to war against him. He immediately set sail and defeated the Persians.



Historical Example 2

- The Greeks also invented a code which changed letters into numbers. A is written as 11, B is 12, and so on. So WAR would read 52 11 42. A form of this code was still being used two thousand years later during the First World War.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

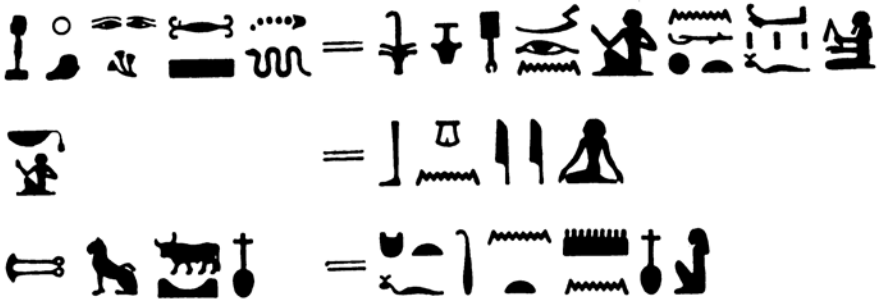
Historical Example 3

- The Roman Emperor JULIUS CAESAR invented his own simple code. He moved each letter of the alphabet along three places, so that A became D, B became E and so on. His famous phrase VENI, VIDI, VICI ("I came, I saw, I conquered") would have read YHQL YLGL YLFL.

years is, in other words, exactly the story of mankind.

China, the only high civilization of antiquity to use ideographic writing, seems never to have developed much real cryptography—perhaps for that reason. Diplomats and military authorities relied mainly on oral statements, memorized and delivered by messenger. For written messages, the Chinese would often write on exceedingly thin silk or paper, which they rolled into a ball and covered with wax. The messenger hid the wax ball, or "la wan," somewhere about his person, or in his rectum, or he sometimes swallowed it. This, of course, was a form of steganography.

Actual cryptography often involved open codes. If a man's name included the ideogram for "chrysanthemum," the correspondents would refer to him as "the yellow flower." But for military purposes, the 11th-century compilation, *Wu-ching tsung-yao* ("Essentials from Military Classics"), recommended a



Hieroglyphic encipherments of proper names and titles, with cipher hieroglyphs at left, plain equivalents at right

true if small code. To a list of 40 plaintext items, ranging from requests for bows and arrows to the report of a victory, the correspondents would assign the first 40 ideograms of a poem. Then, when a lieutenant wished, for example, to request more arrows, he was to write the corresponding ideogram at a specified place on an ordinary dispatch and stamp his seal on it. The general could put down the same character with his own seal to indicate approval, or his seal without the character to indicate disapproval. Even if the message were intercepted, the code portion would remain secret.

It is questionable, however, whether such methods were much used. The greatest conqueror of them all, Genghis Khan, seems never to have made use of cryptography. Nor do ciphers seem possible. The ideographic nature of the language precludes them. The cipher-like technique of altering the form of the ideograms by shifting lines or elements from one place to another in the pattern would be, one authority has said, neither practical nor effective. In fact, one of the apparently few cryptologic episodes in the history of China involves a Western alphabet.

Cryptograms on Gold Bars from China (about 1930's)

Cryptograms on Gold Bars from China (about 1930's)

Cryptograms on Gold Bars from China (about 1930's)

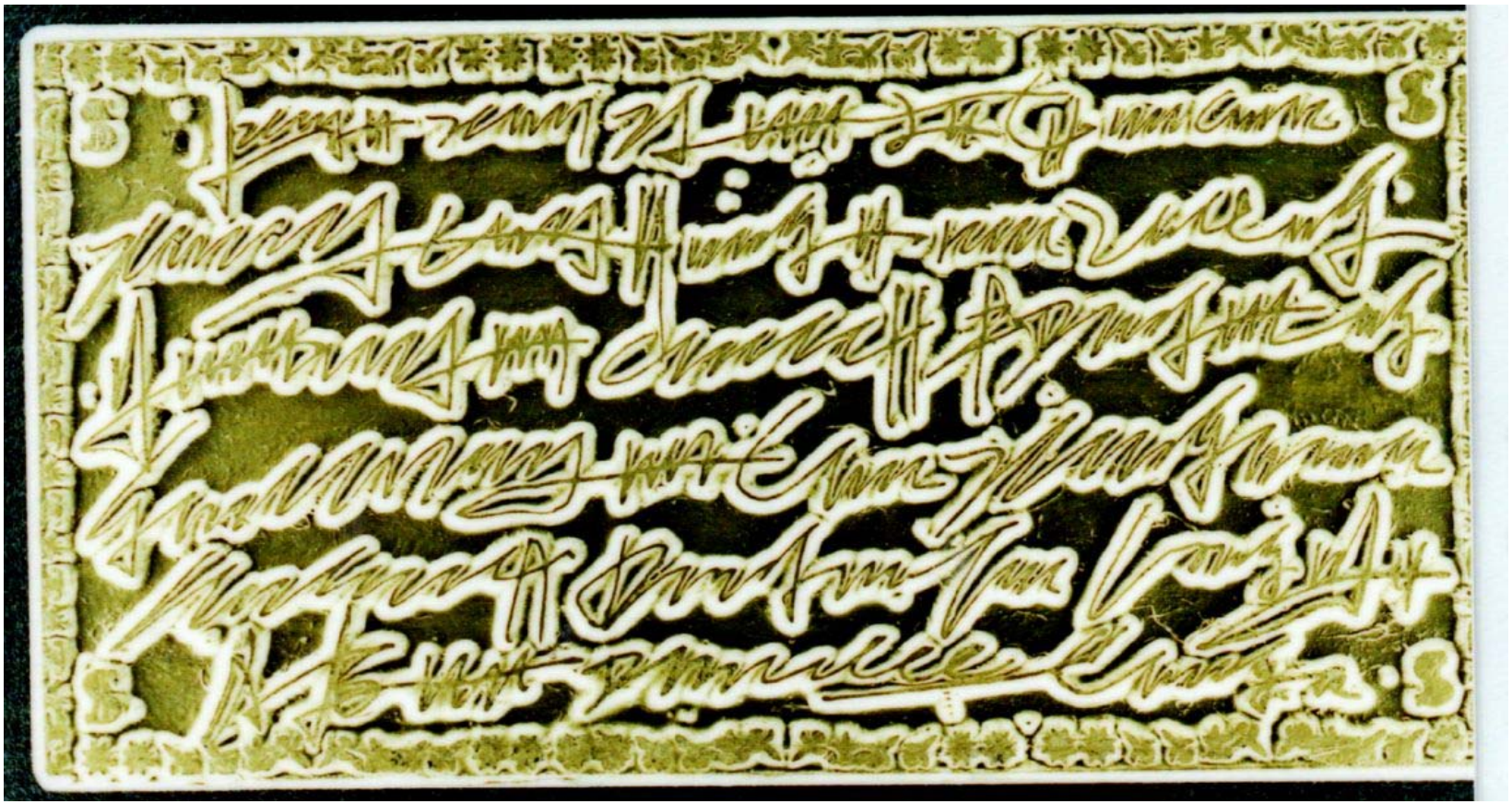
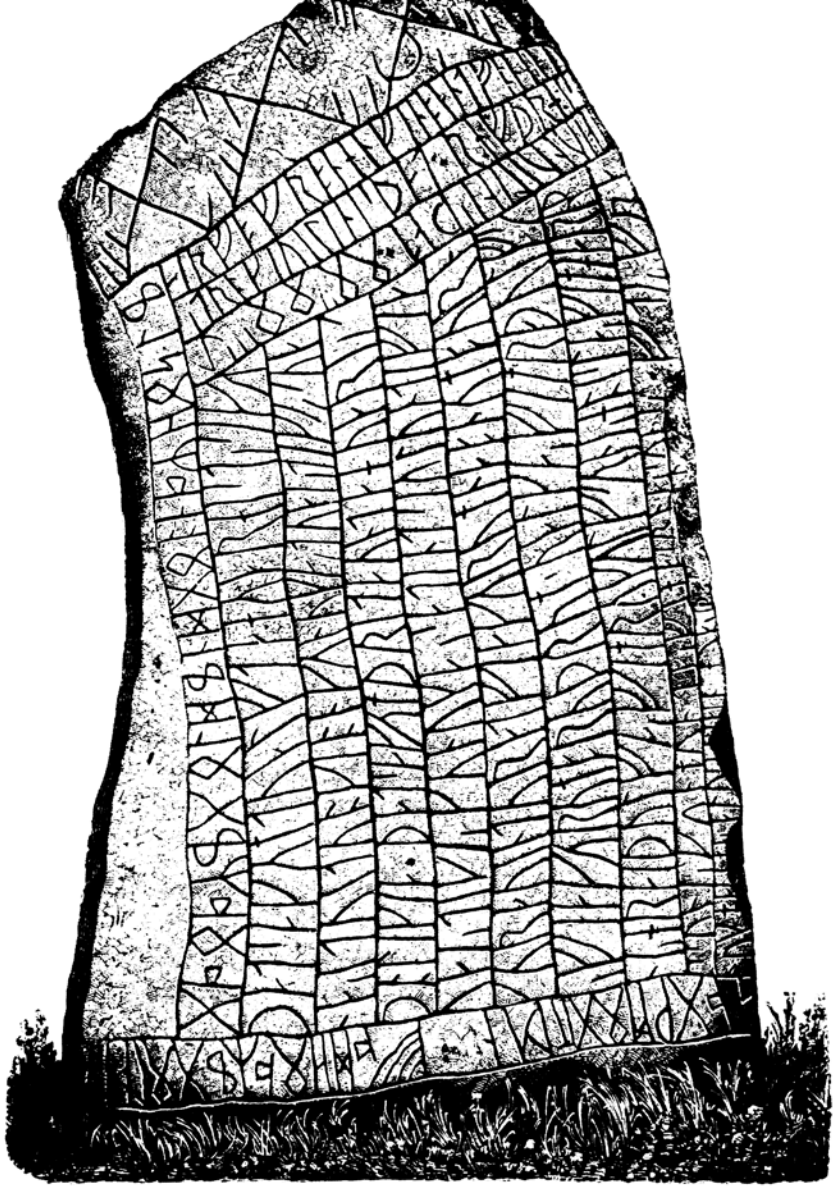


Figure 10. Unknown cipher by Robert Folger, 1827.

[Ed. note: A solution to the above Folger cipher will be published in the July 1983 issue of Cryptologia.]



The 13-foot-high Rök stone of Sweden, covered with enciphered runes

of eight runic letters each. The letter thorn, for example, which looked somewhat like a modern *p* and represented the initial sounds of "thin" and "then," was the third letter of the first group. All systems of runic cryptography replaced runic letters by groups of marks indicating the number of a letter's

would be less likely to lie at the elbow of one of Moriarty's associates. The only volume which fits both requirements is *Whitaker's Almanac*. The current edition yields the senseless *Mahratta government pig's bristles*, but last year's gives perfect sense. Thus Holmes solves the cryptogram purely by use of his famed deductive powers and without really needing to know cryptanalysis.

But his thorough knowledge of that subject, as of all others needed in his chosen profession, becomes manifest in his "Adventure of the Dancing Men." The dancing men—little stick figures with their arms and legs in various positions—constitute the cipher symbols. An American gangster, Abe Slaney, "the most dangerous crook in Chicago," writes threatening notes in them to a former childhood sweetheart, Elsie, who has married an English squire. The squire copies the messages, which are chalked on window sills and tool houses, and brings them to Holmes. Holmes solves them, but the squire is killed by Slaney in an exchange of shots before Holmes can prevent the tragedy. Slaney escapes. Holmes, who knows where he is from the solved

A message in the Dancing Men cipher, solved by Sherlock Holmes

cryptograms, carefully composes a message out of cipher symbols that he has recovered and sends him a note urging him to *Come here at once*. (Holmes perhaps borrowed this scheme from Thomas Phelippes, who, Holmes knew, had in 1587 forged a cipher postscript to a letter of Mary, Queen of Scots, to learn the names of the intended murderers in the Babington plot against Elizabeth.) Slaney, naïvely believing that only Elsie and others of his Chicago gang at the Joint could read the cipher and that the note must therefore have come from her, returns to the squire's home. He is at once arrested and, naturally, confesses.

Holmes is, as he himself says, "fairly familiar with all forms of secret writings, and am myself the author of a trifling monograph upon the subject, in which I analyse one hundred and sixty separate ciphers, but I confess that this is entirely new to me." He referred, of course, to the use of the dancers "to give the idea that they are the mere random sketches of children," and not to their nature as a monalphabetic substitution. That he promptly recognized that they belonged to this class of ciphers is proved by his embarking at once upon a solution without any false starts. His task was considerably more difficult than that of any other fictional cryptanalyst, because his text was exceedingly short, disconnected, and elliptical and loaded with proper names. It eventually consisted of five messages in telegraphic English: (1) *Am here Abe Slaney*, (2) *At Elriges*, (3) *Come Elsie*, (4) *Never*, (5) *Elsie prepare to meet*

Cryptanalysis

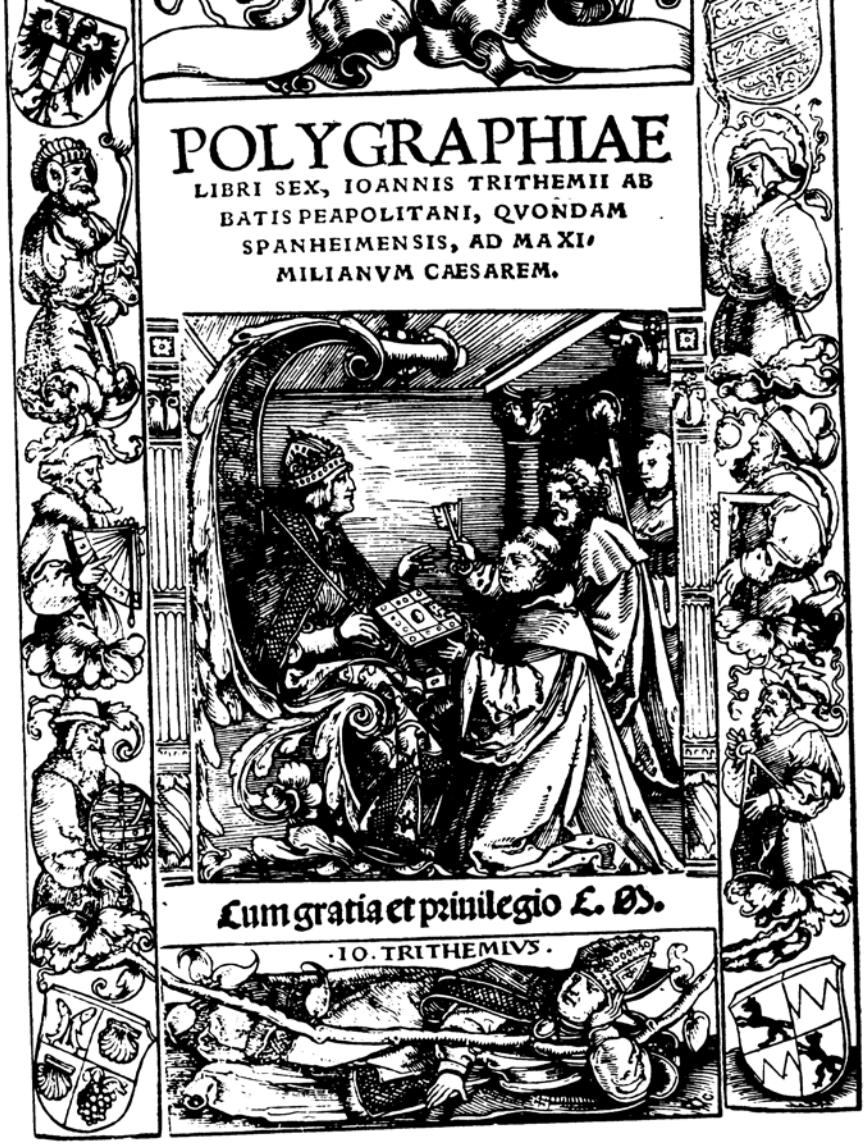
- After the fall of the Roman Empire codes were not used much until the sixteenth century.
- Then Italian and French scholars began to make up very complicated codes.
- The science of code-breaking - CRYPTANALYSIS - had begun.

Cryptanalysis: Example 1

- In Elizabethan England MARY QUEEN OF SCOTS sent coded messages to her supporters who were plotting to murder Queen Elizabeth I.

Cryptanalysis: Example 1

- The messages were intercepted by the head of Elizabeth's secret service, Sir Francis Walsingham. He deciphered them and discovered the plot. Mary was executed for treason in 1587.



The woodcut title page of the first printed book on cryptology. Though taken from an earlier book by the same author, Johannes Trithemius, the illustration was apparently appropriate to this book as well. It shows the author wearing his Benedictine habit and, with his abbot's miter on the floor before him, kneeling to present his book—padlocked, as befits its secret character—to the dedicatee, the Holy Roman Emperor Maximilian I. Seated upon his throne in the imperial castle at Augsburg and wearing the imperial crown and mantle, Maximilian holds his scepter in one hand and blesses Trithemius with the other. Behind Trithemius, another person—either another monk or the publisher—extends towards Maximilian two keys to the book, these symboliz-

numbered lines
typical column
word, HUBON. T
how this was to
artificial words
last letter of the
ECOZACH, ADON

a
b
c
d
e
f
g
h

Th

the second let
from his first
ADAMAI. Onc
Trithemius ju
gives suppose
first printed
It is Book
Here appear
This is the el
once all the
same sequen

*ing Maximil
Trithemius' c
reclines with
its fruits" an
At upper left
at lower left,
anity; the sh
right, arms o
sphere, a sex*