MAKING SECRET CODES

What does this mean: EREH EW !OG ?

Or this: HƎЯƎ YOU ƤO ?

I guess those secret messages were not too difficult to solve. It was only 'here we go!' with words written backwards and in mirror writing. Mirror writing is the first code for many kids, indeed the way many begin to write at all. Have you saved any of your early writing efforts? Did you occasionally write in mirror? One of the most famous mirror writers was Leonardo Da Vinci, the creator of the painting Mona Lisa. He was a technical genius and an inventor asides from being an artist. Because he was left-handed he found it easier to write from right to left.

Writing in secret code is called **coding** or **ciphering**. Each code has a **key**: the key locks and opens the code. The key contains the rules of the cipher, for instance how to replace characters in a message. We start learning secret codes with some easy and well-known ciphers, and later we look at the basics of code cracking. The simplest keys tell how replace a letter with another sign: a letter, a number or something else. This is called simple **substitution**.

Look at the example: Numbers can substitute letters, like in this key:

A	B	C	D	E	F	G	H	I	J	K	L	M
9	3	18	23	7	20	24	10	13	21	16	8	4

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	1	5	11	22	15	19	2	26	17	24	6	12

What is the message: 26 7 22 6 15 7 18 22 7 19 ?

PRACTICE:

All the following codes are simple substitution codes. Read the story with the help of the key below. The story begins like this, and you can cipher the rest.

X+? A/$9 @1& X+? 8+??5

@ A/$9 +@& 4??1 +7~X =1 @ 9=3+X A=X+ @ 4?@~

+? A@8 71@4$? X/ |/;? @1& %/7$& 1/X 8@X=89O +=8 +713?~ @1& X+=~8X

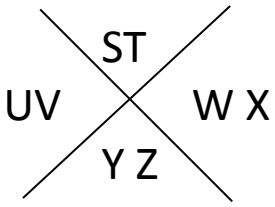
Key :

A	B	C	D	E	F	G	H	I	J	K	L	M
@	4	%	&	?	9	3	+	=	>	<	$	|

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	/	5	2	~	8	X	7	;	A	_	O	š

Pigpen cipher

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



To write on A, indicate the position __| and for B with a dot •_|

The story: "The Wolf and the Sheep"

A Wolf had been hurt in a fight with a Bear. He was unable to move and could not satisfy his hunger and thirst. A Sheep passed by near his hiding place, and the Wolf called to him. Please fetch me a drink of water, he begged; that might give me strength enough so I can get me some solid food. Solid food! said the Sheep. That means me, I suppose. If I should bring you a drink, it would only serve to wash me down your throat. Don't talk to me about a drink! A knave's hypocrisy is easily seen through.

PRACTICE:

Write the rest of the story yourself in the pigpen cipher.

MORE CODING METHODS

TRANSPOSITION

Above we made some secret codes by giving a new sign for each letter. Instead of replacing characters in a sentence, the letters can simply be shuffled. It is called the **transposition** method. For example a transposition of 6 characters means changing the order of (1 2 3 4 5 6) to (5 1 3 2 6 4).

Look at the example:

	123456/123456/123456/123456/123456
message:	let us/ go to/ the p/ark to/night
	513264 513264 513264 513264 513264
in code:	ultes t ogo htpe takro tngi h

Note that the blank spaces are also included.

What does this message say (in the same code):

yaero auc zr y ?

PRACTICE:

Write a message using the transposition method and give it to your friend to solve.

NONSENSE CODE

Here we have a very easy code: just add one nonsense letter in front of each letter in the message. If you leave the word divisions intact, one can quickly see what kind of code you are using. To make it more difficult to detect the code, divide the new text in groups of five-character-words. To read it is just as easy: you only delete every other character. Example:

MARY IS GOOD

SMWAO RKYGI RSHGL OAOTD

PRACTICE:

Solve this message:

wberaortehcerrasz iaensd rseiasdttewrhs ahiafvyeo uIc annornte,

tbhuetw ntehxatt dmaayn'ist rfaaitnheedr viesr ymhye vfialtyhaelrl's dsaoyn

CODE BOOK

Code books can be used in a variety of ways, for example you could design a code book yourself or you could use any book as a source for codes.

The most tedious coding method is to select any book which has much text, and pick up words from that book. Instead of writing the word, note its location in the book: page-row-word. Your friend who reads the message must have the same book. This may be rather time-consuming. Another way is to pick up a key word from the book and use it in other ciphers, like for the Caesar cipher (see below).

Code books were very popular in earlier times. They were used also openly to shorten telegraphic messages to save money. The armies had code books of military operations still in the beginning of this century.

SHIFTING ALPHABETS

A shifting alphabet works like this: replace A with B, B with C, C with D, and so on. "Dracula => Esbdwmb". Here you shift the alphabet just by one position. The code is harder to solve if the characters are shifted farther, for example 4 positions: A becomes E, B becomes F, and so on.

The first emperor of Rome, Julius Caesar, was a successful military commander. He used the shifting alphabet to code his messages, and thus it is still called the Caesar cipher. One may wonder why he was content with such an easy code but at that time it was not a problem. Literacy was not common, and most of his soldiers could not read even plain text!

A more complicated variant of this code is to use a different shift for each word: first select a keyword like ZOMBIE and then use the letters to indicate the shift: Z means that A is replaced by Z, B is replaced by A, C by B and so on. This shift is used for the first word in the message, and again for the seventh word. For the second word, use O as a key. O is a shift of 14 positions in the alphabet: A becomes O, B becomes P, C becomes Q and so on. Look at the example:

key	Z O M
message	MARY IS GOOD
in code	LZQX WG SAAP

To play with this code, make two strips of paper with the alphabet on each strip, and move the other as instructed by the keyword. If the key letter is R, place R under A.

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 A B C D

I

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

When writing the message, replace a letter from the upper row with the character below it. When reading, replace the character from lower row with the letter above it. To keep track where you are, mark the key-letter above each word. This code is a bit hard to operate, but after some practice you will be quick. Best of all, the code is hard to crack!

PRACTICE:

Work with this code. Make two strips of paper with the alphabet on them. Using KEYWORD as the keyword read the message below:

mrkbvso, glevpmi, gl pda hip, tyrczv, fkduolh, zevvon syx rfc lhqc.

cv dp jrrgqhvv, yh qc qmsj, pdana ucsg tyriczv grzq dro lspi.

Select your own keyword, and write a message to your friend to read.

SECRET CODES IN THE REAL WORLD

DISCUSSION:

Who would need secret messages? Secret codes are fun but why would serious adults engage in ciphering?

Secret societies tend to have secret words and symbols which only the initiated members know. There have been secret societies all over the world since earliest times. We know that in some West African religions there are separate secret societies for men and for women. They have different dances, songs, dresses and make-ups, but for important functions they sort of complement each other. Priests from one society are invited to visit rituals of the other society. Likewise, Native American medicine men, or traditional healers, have so called medicine societies. The initiation to a secret society is always a long process which takes years: new members need to learn much concealed information, secret songs, chants and signs before being admitted to the society. They also have to perform tasks to prove that they are worth of the membership: that they

have enough courage and skills.

Famous secret societies existed in the European history, as well, like the Society of Freemasons. Its members were not necessarily masons at all, to the contrary, many famous men - and only men, no women were admitted - belonged to it. They have secret signs, passwords and ciphers: They are told to have used the "Pigpen" cipher which is also called "Masons' cipher". (Look at the story in the beginning of this chapter.)

Criminal societies, in particular, keep their secrets tightly guarded. It is no wonder that there is not much public information about these societies or their codes. Yet some examples are known like the secret language of thieves in London from the 19th century, the smugglers' language from Germany, and the language of street vendors in Bombay, India. The thief talk of London is presented later on page 14.

Foreign and intelligence services are, of course, frequent users of ciphers. They employ tens of thousands of mathematicians in cryptography and code breaking. Diplomats, spies, and military personnel are all coding the messages they send to their superiors, and field workers get the instructions in coded form. Major war operations and missions have code names. Similarly, computer industry gives code names for products which are under development.

CRYPTOGRAPHY AND THE BREAKING OF SECRET CODES

CRYPTOGRAPHY

The military used to have code books which included lists of actions and words and codes for them. Those codes were hard to keep secret and they became completely useless after once deciphered or found by the enemy. More complicated methods were developed in the 19th century. Ciphering became more and more based on mathematical methods: a letter has first to be turned into a number, and that number is then multiplied, divided again and so on according to the rules of the method.

The Second World War 70 years ago was very much an intelligence war. All sides depended heavily on radio communications, and they had to develop advanced codes to keep the messages secret. Many leading mathematicians and linguists were employed in code-breaking during the war, numbering 30,000 in Great Britain alone. Japan had invented an advanced coding machine which they believed to be impossible to crack. The Allies succeeded in breaking its code which of course was to be kept secret. But a newspaper, The Chicago Tribune, published the news however because it was against the war. The Japanese refused to believe this for their misfortune, and continued using the code during the war. Thus the Allied Powers were aware of their strategies in advance and could be prepared for attacks.

Mathematical methods are exclusively used in modern ciphering. The calculations are so complicated that computers are needed to perform them. Banks and big companies need hidden codes to keep money transactions secure. Computer messages about money are all ciphered and sent in a coded form. As you may know, every computer user and bank card user needs a password or identification number to be able to give instructions to the system like when asking for money withdrawal or transfer.

EXAMPLE:

A bank card has a personal secret number. Before you are able to use the card, you must enter the four numbers correctly. If you forget the number, how easy is it to guess right? The first number can be any of 0 to 9, your chances are 1 out of ten. The second number has also 10 different alternatives, that makes ten times ten which is a hundred. For each of those hundred

possibilities, there are ten different third numbers. We get one thousand possibilities. A fourth number makes the chances to hit right to one out of ten thousand. Because the numbers are selected arbitrarily, nothing helps in guessing. Think of the possibility of using one's first name as password. Would it make guessing the right password easier?

Practice: make a PIN code guessing game. One person writes a four number code on paper without showing it to the others. First player guesses a number which is written for all to see. The game leader marks correct digits: a hit in the correct place is marked with a circle and a correct number in wrong position is underlined. Write rules for the game and play it in a group.

HOW TO BREAK CIPHERS

A code is secret only as long as outsiders are not able to read it. Would it be possible to design a code which is impossible to break? This is the big question of cryptography, the science of secret codes. Every code must have a system: there are rules how to write the code and reverse rules how to read the code. Is it possible to develop a rule which nobody would find out? Or could one invent a key which cannot be found? Let us take a look at code breaking, and return to our question afterwards!

You may have already realized that many secret codes are not that difficult to break at all. We started our secret writing with simple substitution codes. They are easy to use, and also among the easiest to solve. They can, in fact, always be cracked. One starts by examining the pattern of sign combinations, and making guesses. If word divisions are indicated, are short words the first targets. If there is a one-letter word, what could it be? (There are only two alternatives.) You make a guess and test how it works in the text.

You know that all words have vowels in them, and you can try to locate vowels first. Some letters occur in written English much more often than others. The most common letter in English texts is E, and then come T, A, I, N, O and S. The letters which occur rarest are X, Z, J and Q.

Statistics gives us another clue also: the frequency -how often they appear- of words in normal English text has been counted from a large amount of books and articles. You can use the results when trying to break a code. The twenty most common English words are, starting from the most popular:

the, of, to, in, and, a, for, was, is, that, on, at, he, with, by, be, it, an, as, his.

PRACTICE: DECIPHERING CODED MESSAGES

PROBLEM 1:

Find the code (make a key chart) by concluding which word matches the words in code. The code is made of numbers: one number for each letter. Here is a set of words in code, find matching pairs:

24 6 25 2	MOON
16 18 18 26	THAT
24 6 15 24	THIS

Key chart: fill in letters from above:

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

Five more words are:

HERE	14 9 8 8
WELL	19 15 13 9
FARE	6 9 13 9
PURE	22 18 26 9
CONE	10 3 13 9

You may now be able to solve the remaining words without hints. Use the key and guess the few missing characters:

19 15 24 6 9 13

2 25 2 24 9 13

4 13 18 24 6 9 13

16 18 16

2 3 26

16 3 16 16 20

22 8 18 3 1

PROBLEM 2:

The letter statistics could be successfully applied to all kinds of simple codes where a word is always coded the same way. The coded text has to be longer than a couple of words, of course, otherwise there may be many possible solutions.

1 2 3 4 5 6

How many solutions can you think for the code above?

(examples: garden, fathom, bright, couple)

COMPUTER CRYPTOGRAPHY

Computer cryptography uses mathematical formulas and large numbers to generate secret codes. Some methods use complicated calculations for encoding and decoding. Other methods calculate the key anew for each character and each number every time they occur, using randomly selected large numbers.

Prime numbers are used in the most efficient encryption methods. A prime can be divided only by itself and one. The smallest primes are 1, 2, 3, 5, 7, 11, 13, and 17. Because primes have no other factors they are more difficult to manipulate than other numbers.

In summer 1993, a group of Internet users joined their efforts in breaking a famous number, RSA 129, which has 129 digits. It was an example of an 'unbreakable' key for encoding. It is the result of two large prime numbers which were kept secret. The number RSA 129 is known, and anybody could use it for encoding a message. But only a person who knows its factors, those two primes, can crack the message. A huge amount of calculations are needed to find the factors of a large number, in fact so many, that it was considered impossible to break RSA 129 because it would take millions of years for a computer to perform the calculations. The cryptography group in Internet realized that they can divide the job in smaller parts and use many computers at the same time to attack the problem. It still took a year for hundreds of computers to find the factors, but the effort proved that 129 digits are not enough to make a key absolutely secure. Experts now believe that a number which has no less than 230 digits is needed as a key if one has to sure that it cannot be cracked for some more years.

PRACTICE:

Continue the list of prime numbers.

PRACTICE 2:

Doing statistics: count the frequencies of words in sample texts. Select blindly a page number in a book (for example page 37) and count how many times common words occur on that page in different books. Look at the words given above (the, of, to, in, and). Do you get same words as in general statistics many times or are some other words more common? If there is a difference, what would be the cause?

UNBREAKABLE CIPHERS

There are some secret codes which are so strong that they cannot be broken. The cipher developed by Gilbert S. Vernam is assumed to be one of them because it uses a 'one-time' system. The key is changed for each message, and never repeated.

A paper-and-pencil version of a 'one-time cipher' works as follows. There are actually two keys: one to transform letters into numbers, and a second key which is a series of arbitrary numbers. The only way to reveal the message is stealing the keys. The cipher works like this:

Step 1: Letters are changed into numbers (key 1).

Step 2: Numbers are added to another secret set of numbers (key 2). If the result is larger than ten, only the number for ones is written in the code. This produces a third set of numbers which is the secret message. The message could be sent by radio or by mail.

Step 3: The receiver can read the message by subtracting the key number 2, and the again transforming the numbers back to letters (key 1). Because word divisions are not marked, they must be guessed.

Example key 1:

A 6	E 8	I 39	M 70	Q 71	U 52	Y 1
B 38	F 30	J 31	N 76	R 58	V 50	Z 59
C 32	G 36	K 78	O 9	S 2	W 56	
D 4	H 34	L 72	P 79	T 0	X 54	

Message: I L I KEYO U.

Coded 1: 3972397881952

Numbers: 752964023875427 6157754207689

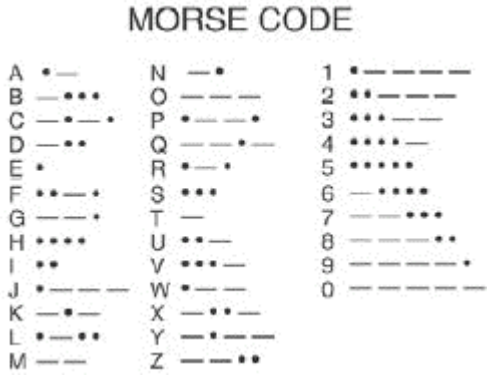
Addition: 0491937019606 This is the message.

Look at the first number on 'addition' row. It is the last number of the result of 3+7, namely 0, the 1 of 10 is discarded. When you decode the message, you have to subtract 7 from 0, and then you again make it 10 in your mind: 10-7 =3. Because there is no 3 in key #1, you must calculate the second number 4-5, or 14-5=9. Now you have 39 which is 'I'. And so on.

CHAPTER 4: TRAVELING SIGNALS: MORSE CODE

.../---/...

SOS = "Save Our Souls" is an international message of distress. Wherever you happen to be, if you need help you can send the SOS-signal. It is expressed with three short signals followed by three long signals and again three short signals in Morse code: .../---/... Long and short signals could be made up in a variety of ways: as sounds, as smoke signals, or as flashes of light.



Discussion:

How do you communicate, if you want to invite a friend from another town over for the weekend? Which are the fast ways and which are slow?

Before there were any modern communication means like telephones, messages had to be somehow carried to the receiver. It usually took a long time before a message reached the receiver. Likewise traveling took long as well, and if people went for a visit, they did not return soon. Visiting relatives could easily stay weeks or months.

Messages were written on letters and carried by mail wagons, runners, horseback, or ship.

Sometimes faster methods were used, like trained pigeons to bring airmail. There were also some clever ways to send emergency calls: Native Americans sent smoke messages, and Africans used drumming. When Troy had fallen to the besieging Greeks, they sent runners to bring torches to their home cities.

Samuel F. B. Morse invented the telegraph in 1835. That was the first time when signals could be sent very fast over long distances. Soon afterward he developed a code for standard communication which was then called Morse code. Telegraph machines were connected by electrical wires and they transmitted short and long impulses, taps, from one end to the other. As electric signals travel almost as quickly as light, they reach the other end in an instant. Sixty years later a young Italian, Guglielmo Marconi, developed a wireless telegraph, using radio signals.

PRACTICE:

Find the answer:

What's yellow and fuzzy and goes up and down?

.-//.--./.-/-.-./….//../-.//.-/-.//./.-.././…-/.-/-/---/.-.//

What's long, orange, and wears diapers?

.-//-…/.-/-…/-.--//-.-./.-/.-./.-./---/-//

PRACTICE

Try to tap Morse code with your fingers and hand, or with a keyboard. Make a short break after each character. Note, how fast it is!

Play games with Morse code: One person sends a message by whistling, and others compete in catching it. Everyone has a pack of Morse cards, and picks up the letter which was whistled. Who is first? To make it more difficult: one sends a word in Morse code, and the one to solve it first is winner.

A SECRET LANGUAGE: THIEF TALK from old London.

Thief talk was a secret language used by street criminals in London during the 19th century. They did not want the police, or anybody else for that matter, to understand what they were talking about. Using a secret language they were able to exchange information and to recognize each other. The knowledge of secret language was also sort of prestige for anyone on

the streets: he showed that he is one of the tough guys.

It has been difficult to study that language because the thieves themselves never revealed meanings of words, and those who knew secret words were sworn to keep their mouths shut. This much is known:

Thief talk	plain English
Anna Maria	fire
apple pies	eyes
blunt	money
Brown Bess	yes
Brown Joe	no
buffer	watch-dog
croaksman	murderer
forks	fingers
to fox	follow
Frank and Hank	bank
frog and toad	road
greasy chin	child
half a tick	sick
to knuck	to pick pockets
mang	to talk
moan and wail	jail
outer	thief
plates of meat	feet
pop	pistol
pride and joy	boy
Rory O'More	door
to scroll	to write
skin	shirt
to souse	to eat

tog	coat
Tommy	bread
twist and twirl	girl
What circle?	What time is it?

PRACTICE:

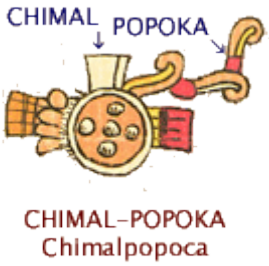
This is a story in thief talk, translate it into English:

This morning I felt *half a tick* and my *plates of meat* were aching. But had to go *to knuck* to get some *blunt* because I wanted *to souse* some *Tommy*. So I put my old *tog* on and took a *pride and joy* along, and we went near the *Frank and Hank*. But there was a *twist and twirl* who knew that we are *outers*, and she went to *mang* to other people. The *pride and joy* said that he doesn't want to go to *moan and wail* and went off, and I *foxed* him.

KENNINGS

In fact, some of words in the thief talk are so called kennings, or roundabout expressions for unpleasant things, like "moan and wail" for the prison and "buffer" for a watch-dog. But secret language and kennings are not only for outlaws. Sometimes they distinguish nobility from commoners like in the ancient Mexico. The Mixtec, who lived in the mountains of Central Mexico, used to call ordinary people "the earth people". The commoners could not speak the true, noble language of the kings. The nobles, on the other hand, were descendants of the gods, and they said that they had descended from trees. They used a special language called 'iya' dialect which was full of metaphorical expressions. When a commoner was said to die, a noble just 'fainted'. Commoner women nursed their babies with milk but noble women had 'honey' in their breasts. And when a commoner simply urinated, nobles 'made dew'. Also the body parts of nobles had different names than in case of commoners.

Among the Maya in Yucatan, only those nobles who knew a secret language called Zuyua were allowed to be chiefs. Village chiefs had to pass an examination of noble speech which was conducted by the highest priests. The high priests gave them riddles in Zuyua language to find out if they really were of noble family. Only sons of chiefs could had learned the secret knowledge from their fathers.



Picture: Aztec name for smoking shield

The Aztecs, who also lived in Mexico, had kennings for important, powerful things:

arrow and shield	= war
rope and cord	= war
throne and mat	= power
sun and moon	= beginning and end, thus all time
heaven and earth	= up and down, thus all space

You probably know some words which you are not supposed to say. Those are forbidden or taboo words. 'Taboo' comes from a Polynesian word 'tapu'. It means something forbidden, or something which has so much magical power that ordinary people are not allowed to touch it, or even to see it. The traditional kingdom of Hawai'i was the most famous Polynesian society. Ordinary people were under many taboos in Hawai'i, for example they were not allowed to look at their queens or kings. If they were caught watching the king, they could be punished with death. On the other hand, it was perfectly acceptable to sing the praise of king's private parts. Words which are taboo for you, were not taboo for the Hawaiians. They had taboo words, too, but those were about origins and families of the rulers. Only the highest priests were allowed to tell the family history of the king.

In old times, some things or animals were considered too dangerous or too powerful to be named directly. In English the words 'bear' and 'beaver' mean originally 'the brown animal'. The people were afraid to say the real name of a bear when there still were many bears in the forests. It was believed that the bear is very mighty and can hear and see everything. People lived much closer to the nature, and they had to take it into consideration. Most of the people lived in small villages which were surrounded by forest.

The hunters in Siberia think that the bear has magical powers. When a bear has been killed, she is sent back "home" to the heaven with a big feast. People send messages to their ancestors spirits in the heaven together with the bear's soul. If the hunters do not talk respectfully about the bear she may get angry and refuse to help them. That's why they use a secret language when hunting, and call animals by all kinds of nicknames.

In many places it is not considered proper to mention the names of persons who have recently died. The spirit of the dead person is thought to be still nearby, and people do not want to disturb it on its way to the Other World. When a person dies, her namesakes may even have to take a new name. The aboriginal people of Australia have that custom. Their religious system is very complicated, and it includes many taboos. It is taboo to say the name of a recently died relative. For a husband, it was forbidden to go near to his mother-in-law or to talk to her. Some Australian aborigines have developed a sign language to avoid this kind of word taboos. Things what they are not allowed to say they can sign with their hands. There are old women who have lost many relatives, and who have stopped talking at all. Their sign language is so advanced that they can sign whatever they want to say.

The Native peoples of North America had a fully developed sign language, as well. It is called Plains Sign Language because it was mainly used in the Great Plains area. This sign language was used in communication between people who did not know each other's languages, for example among travelers or in big gatherings of many tribes. It was very useful because there were numerous indigenous languages in America. The Sign Language was also used by storytellers or just for fun in a camp. Some signs were easy to understand: two hands bent upwards on temples meant buffalo (horns), and a hand movement towards mouth meant eating.

Similarly, the Christian Trappist monks have made a vow to be silent. Yet in their daily work they need to communicate somehow. For this purpose they use hand signs which are related to the work, for example to beekeeping.