Secret Codes and Cyphers

UWSP College Days for Kids
Spring, 2021
Dr. Andy Felt, leader

Welcome to the session on secret codes and cyphers. Cyphers are used when you want to write a message to someone and keep others from reading the message. There are three skills associated with cyphers and codes.

1. Writing the message is called *encoding*.
2. Reading the message is called *decoding*.
3. Trying to read the message when you don't know how it was encoded is called *breaking* the code.

Which of those three skills seems the hardest? We will start with some simple cyphers and build up to more advanced cyphers.

1 Substitution Cyphers

In substitution cyphers, each letter is represented by a different letter in the code. So, for example, we might have the following substitution scheme:

real letter	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
coded letter	k	j	i	h	g	f	e	d	c	b	a	z	y	x	w	v	u

r	s	t	u	v	w	x	y	z
t	s	r	q	p	o	n	m	l

If we want to encode

$$\mathsf{CAT}$$

we look up the letters C, A, T in the "real letter" row and see that they correspond to the letters I, K, R. So

$$\mathsf{CAT} = \mathsf{IKR}$$

Exercise 1 Use the substitution scheme above to encode this message:

j o i n t h e u l t i m a t e

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _

f r i s b e e c l u b

_ _ _ _ _ _ _ _ _ _ _

Exercise 2 The substitution scheme above (a=k) was used to encode this message. Decode it.

o k m r w e w

_ _ _ _ _ _ _

2 Variations on Substitution Cyphers

There are many ways to make substitution cyphers more complex and harder to break. You don't have to have A=K every time. You could let A=V if you want, or any other letter. This is called changing the *substitution key*. The cypher disk can help you change the key. Let the outer letters be the real letters and the inner letters be the coded letters. Notice that the inner letters go around counterclockwise, while the outer letters go around clockwise.

Exercise 3 Line up the outer A with the inner X on your cypher disk. Use that key to decode this message.

R G T X E O J W

_ _ _ _ _ _ _ _

One way to make your cypher harder to break is to change your key as you write the message. So, you might decide to use A=X for the first line, A=Q for the second line, and A=H for the third line. Or you might change the key after every word, or even every letter! Of course, the person receiving the message will need to know how you changed the key.

Exercise 4 Encode the message, "Green Bay Packers" using the cypher disk. Use A=X for the first word, A=Q for the second word and A=H for the third word.

g r e e n b a y p a c k e r s

— — — — — — — — — — — — — — —

Exercise 5 Decode the following message using the cypher disk. The first word uses the key A=X. The second word uses the key A=(the last real letter of the first word). The third word uses the key A=(the last real letter of the second word).

T A T G V P F T A J A N G V Y A

— — — — — — — — — — — — — — — —

3 Polyalphabetic Substitutions

A cypher method that is very difficult to break is a polyalphabetic substitution. Here is one:

	B	L	A	C	K	H	O	R	S	E
B	a	b	c	d	e	f	g	h	i	j
L	k	l	m	n	o	p	q	r	s	t
A	u	v	w	x	y	z	a	b	c	d
C	e	f	g	h	i	j	k	l	m	n
K	o	p	q	r	s	t	u	v	w	x
H	y	z	a	b	c	d	e	f	g	h
O	i	j	k	l	m	n	o	p	q	r
R	s	t	u	v	w	x	y	z	a	b
S	c	d	e	f	g	h	i	j	k	l
E	m	n	o	p	q	r	s	t	u	v

Notice that the letter "a" shows up four times in the table. If I wanted to encode an "a", I could use (B,B) or (A,O) or (H,A) or (R,S). This makes it much harder to break, because common letters don't show up as easily.

Exercise 6 Decode the following message using the BLACKHORSE table.

(C,O) (H,O) (B,K) (E,C)

— — — —

(C,C) (S,A) (R,S) (C,R) (K,H) (H,E) (A,K)

— — — — — — —

Notice that even though the letter "e" was used three times in that 11 letter message, it was encoded three different ways. That's the advantage to this method.

4 Fun Codes

Some codes are not so serious. For example, the shopping list code is a fun one. The number before each item tells you which letter to take from the word. For example, "2 steaks" means the letter "T", since that is the second letter of the word "steaks". The code "5 steaks" would mean the letter "k".

Exercise 7 Decode the following message written using the shopping list code.

2 eggs
3 noodles

5 tomatoes
2 milk
6 sausages
3 bread
5 pie crust
3 mushrooms

5 Breaking Substitution Cyphers

If you find a message that is written as a simple substitution cypher, there are some things you can do to try to break the code.

- The most commonly used letters in written English are usually: e, t, a, o, i, n, and s, in that order. Count the number of each encoded letter and see if it makes sense to assign "e" to the letter that appears most often. The longer the message, the more reliable this becomes.
- A one letter word will usually either be "I" or "a".
- Look for repeated pairs of letters that might be "th" or "sh".
- Think of common two letter words: "an", "it", "as", "in", "on", etc.
- Trial and error is sometimes required. To avoid erasing a lot, use a helper like at Hal's Cryptogram Helper: `http://www.hjkeen.net/htoys/cryptogm.htm`.

Exercise 8 Try to break the following encoded message. It uses a simple substitution cypher.

j b d f s r s u h n b b f n y r o m

c x n m f s d b f y b f c , e l m j b

d f s n b b q u b s m h m y b o b

m y f m s b b c n m r e b c r s b .

- f u f s m l o x s z

Exercise 9 Here's one for the experts. The wheel will not be helpful here.

e y q j x l o t l b n a k u k

— — — — — — — — — — — — — — —

t l n a k z x z k w l k x w n a k

— — — — — — — — — — — — — — — — —

j y d t j u

— — — — — —

Exercise 10 Here's another message encoded with a simple substitution. Again, the wheel will not help.

b o d d b j u x z o q q n g o e r y b t u j

— — — — — — — — — — — — — — — — — — — — — —

k n e y u o q p u i y o z u o d v u y .

— — — — — — — — — — — — — — — — — — — — —

- e u y d n w o d a f r x

— — — — — — — — — — — — —

6 Want to read more?

You can read about real algorithms used for high level cryptography at Bruce Schneier's blog: `http://www.schneier.com/cryptography.html`. My favorite is the Solitaire algorithm.