Encryption

Part 1.

Alice wants to send a secret message to Bill. Eve wants to read this message. Alice writes the message on a piece of paper and puts the piece of paper in a box. Then she puts a padlock on the box and sends it to Bill. Eve might be able to intercept the box but she can't open it as she does not have a key to the padlock. Bill receives the box and unlocks the padlock with his key. Alice and Bill will have to make arrangements, in advance, so that they each have a copy of the padlock key.

This example is a bit like private-key encryption.

Private-key encryption

Alice wants to send a secret message to Bill using email. Eve wants to read this message. Alice decides that she can't prevent Eve intercepting the email but she can prevent Eve reading the message. She can use encryption.

We will look at two private-key encryption methods - substitution and addition. In both methods, each letter in the message is replaced by a different (or perhaps the same) letter.

1. Substitution

Example 1

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

Method: replace a letter in the top row by the corresponding letter in the second row

Key: the above table (we could use any rearrangement of the alphabet)

We will assume that Eve knows the method being used but she does not have the key.

The message Alice wants to send is: meet me tonight

message	M	E	E	T	M	E	T	O	...
encryption	X	Q	Q	V	X	Q	V	B	...

EXERCISE 1

Alice encrypts a message using the above key and sends it to Bill.

Bill receives: VFQXBRQUIOIRVFQOFQK

Can you decrypt this message for Bill?

Alice and Bill will have to make arrangements, in advance, to use substitution encryption and to agree on the key. How are they going to do this?

There are $26!-1$ different ways we can rearrange the letters of the alphabet, so there are $26!-1$ possible keys. Eve might not be able to try all these keys. However this method of encryption has a serious flaw. Every time there is an A in the message it is replaced by a G in the encryption. Every time there is an B in the message it is replaced by a C in the encryption …etc

This means that Eve can use frequency analysis.

In a piece of text, written in English, some letters will appear more often than others.

The list of letters in order of how often they appear is roughly:

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

So Eve can count how many times each letter appears in the encryption. The letter with the highest frequency will probably correspond to an E in the message. The letter with the second highest frequency might correspond to a T or perhaps an A … etc

This technique works well for long messages.

2. Addition

How do you add two letters? What is $P+U$?

We give each letter a number:

$A=0 \quad B=1 \quad C=2 \quad D=3 \quad \ldots \quad Z=25$

and then add the numbers, mod 26 (see chapter, Modulo Arithmetic)

So $P+U=15+20=35=9=J$

Or we can use a Vigenere square (see footnote)

We can use this idea for encryption.

Method: add the letters of the message to the letters of the key

Key: see examples below

We will assume that Eve knows the method being used but she does not have the key.

The message Alice wants to send is: meet me tonight

Example 2

key: D (we could use any letter)

message	M	E	E	T	M	E	T	O	...
	12	4	4	19	12	4	19	14	...
key	D	D	D	D	D	D	D	D	...
	3	3	3	3	3	3	3	3	...
addition	15	7	7	22	15	7	22	17	...
encryption	P	H	H	W	P	H	W	R	...

Example 3

key: ERIC (we could use any word)

message	M	E	E	T	M	E	T	O	...
	12	4	4	19	12	4	19	14	...
key	E	R	I	C	E	R	I	C	...
	4	17	8	2	4	17	8	2	...
addition	16	21	12	21	16	21	27	16	...
encryption	Q	V	M	V	Q	V	B	Q	...

Example 4

key: GEUKAQPTY (we could use any random list of letters)

message	M	E	E	T	M	E	T	O	...
	12	4	4	19	12	4	19	14	...
key	G	E	U	K	A	Q	P	T	...
	6	4	20	10	0	16	15	19	...
addition	18	8	24	29	12	20	34	33	...
encryption	S	I	Y	D	M	U	I	H	...

EXERCISE 2

Alice encrypts a message using the key: DRMPKZTQDF and sends it to Bill.

Bill receives: IIQSSRTISD

Can you decrypt this message for Bill?

Alice and Bill will have to make arrangements, in advance, to use addition encryption and to agree on the key. How are they going to do this?

Some comments:

Example (2) is known as Caesar encryption.

There are only 25 possible keys. Eve could easily try them all, so this method is a bit rubbish.

Example (3) is known as key-word encryption.

The first E in the message is replaced by a V in the encryption but the second E in the message is replaced by an M in the encryption. This gets around the problem of frequency analysis.

Unfortunately, there are clever statistical techniques that Eve can use to find the length of the key-word. If Eve has discovered that the key-word is four letters long then:

1st, 5th, 9th, 13th, … letters of the message have all been added to the same letter (in my example, E)

2nd, 6th, 10th, 14th, ...letters of the message have all been added to the same letter (in my example, R)

etc

So Eve can now do a frequency analysis on the 1st, 5th, 9th, 13th, … letters of the encryption.

Then Eve can do a frequency analysis on the 2nd, 6th, 10th, 14th, ...letters of the encryption.

etc

Example (4) is known as one time-pad-encryption.

Imagine a note-pad. On each page is a random list of letters. You use the letters on page one of the note-pad as the key for your first message. You use the letters on page two of the note-pad as the key for your second message. etc Every time you encrypt a new message, you use a new page of random letters. As the lists of letters in the note-pad are random then the string of letters in the encryption is random and the encryption is uncrackable.

Part 2.

Alice wants to send a secret message to Bill. Eve wants to read this message. Alice writes the message on a piece of paper and puts the piece of paper in a box. Bill has lots of identical padlocks which he makes available to anyone who wants to send him a message. There is just one key that fits all these padlocks and Bill has got it. Alice gets one of these padlocks and puts it on the box and sends it to Bill. Eve might be able to intercept the box but she can’t open it. Bill receives the box and unlocks it with his key. Alice and Bill do not have to make arrangements, in advance. Anyone can send a message to Bill.

This example is a bit like public-key encryption.

Public-key encryption

Example 5

RSA encryption

Bill picks p and q where p and q are two different prime numbers.

Bill picks e where e and $(p-1)(q-1)$ have no common factor.

Bill solves $ed=1, mod(p-1)(q-1)$ to find d

Bill publishes the numbers e and pq in a public directory for all to see, but he keeps the number d secret.

for example:

Bill picks $p=5$ $q=11$ as 5 and 11 are two different prime numbers.

Bill picks $e=7$ as 7 and 40 have no common factor.

Bill solves $7d=1, mod 40$ to get $d=23$

Bill publishes the numbers 7 and 55 in a public directory for all to see, but he keeps the number 23 secret.

Alice wants to send a message to Bill. She looks-up the numbers e and pq in the public directory. She uses these numbers to encrypt her message.

(don’t worry about how she does this)

When he receives the message, Bill uses the number d to decrypt it.

(don’t worry about how he does this)

Eve intercepts the message. She knows the numbers e and pq because she (like anyone-else) can look them-up in the public directory.

But she needs to know p and q so she can solve $ed=1, mod(p-1)(q-1)$ to find d

So Alice’s message appears to be safe, unless Eve can factorise pq to find p and q

If p and q are large enough then factorising pq will be difficult.

Now don’t worry about the details! Here are some important points:

a) With private-key encryption, Alice and Bill need a way to get together, in advance, and agree upon a key. With public key encryption, anyone can send an encrypted message to Bill. Even someone Bill has never met.

b) The security of RSA encryption relies on the difficulty of factorising large numbers.

c) RSA encryption enables you to buy stuff online. I type-in my credit card number and this is encrypted. Anyone can do it.

d) How does Bill know that the message really came from Alice?

e) My example with $p=5$ and $q=11$ is to illustrate the method. In practise Eve will be able to factorize 55. But if p and q are hundreds of digits long then Eve has a problem.

Encryption is used …

when you withdraw money from a cash machine
when you send messages over the internet or a mobile phone
to protect business and military secrets
in banking
for data storage
for data transmission
for on-line shopping etc

A lot has been written about the use of encryption during the Second World War. In particular, the use of the enigma machine. Read the books. Watch the films. Visit Bletchley Park.

SOLUTION 1
THE MONEY IS IN THE SHED

SOLUTION 2
FRED IS A SPY

footnote

Vigenere square

To find P+U, find the intersection of the P row and the U column. P+U=J

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