Encryption and Decryption: The Science of Secret Messages

Module Plan by Damian Smith, 2005

Summary

This module introduces the idea of writing in secret messages along with its historical and current importance in the world. Several different techniques for creating secret messages (encryption) and also for decoding them (decryption) are shown.

This plan was presented by Damian Smith during UAS 2005, Zambia. It hasn't been seen yet in Kenya so this record serves as both a proposal for this year's module and also for use in Cosmos' database of modules.

The module is fairly well divided into blocks of information and activity so one can stop at any time making it ideal for expansion.

It is heavily based on information found in Simon Singh's "The Code Book".

Target audience age group

8-18.

The material is flexible enough to allow reduction/expansion to cover this age range.

Materials required

The pages at the end of this document should be printed out.

One copy of the large, fixed cipher wheel.

Several copies of the cipher wheels will be needed (two or three copies). They need to be cut out and the smaller disc pinned to the centre of the larger disc with a split pin so that it is free to rotate (not too loosely) and the letters on the inside disc can align with those on the outside disc. Gluing the larger disc to cardboard will help aid longevity!

Several A4 plastic wallets.

Cardboard (just less than A4) – one per plastic wallet.

Whiteboard marker.

Using the cardboard to stiffen the plastic wallets, put one of each of the text based sheets on each side of the wallet so that it can be used as a small, portable whiteboard.

Session plan

1) Introduce yourself and tell the students they are going to learn about two new areas of science called "Cryptography" and "Cryptanalysis". *If they are following the three rules then one of them will ask what these words mean. It is unlikely that this will actually happen so remind them of rule number two – when one of them now asks you can explain that the words mean "Hidden Writing" and "Analysing Hidden Writing".* To set the scene, you can tell them that these sciences have existed for almost as long as people have been writing.

2) Show them the first of the sheets with secret writing on it (marked C3 for "Caesar 3-shift" in the corner). Ask if any of them can read it to you. Explain that the "slash" indicates a break between words. Once they've had a giggle at trying to pronounce, "ZLPJLP BARZXQFLK," tell the students that you've written it in a secret code. It is two English words, but written using Cryptography.

3) Ask if they want to know what it says. You can now reveal to the students the large, fixed wheel. Look at it with the students – point out the main features ***with them***:

    1. The alphabet written in small letters around the outside.
    2. The alphabet written in capitals around the inside.
    3. The inside alphabet is moved round by three places.
    4. The letter "A" is marked with a dot to help us find the letters we want.

    Ask for a volunteer to come and hold the large wheel where all the students can see it, making sure that your helper keeps his/her fingers clear of the letters. Describe how to decode the message they must look for each letter of the secret message (sometimes called "cipher text") on the inside wheel and read the small letter just outside it. So 'Z' Becomes 'C'. Now let them call out each letter and write on the plastic wallet underneath the cipher text in lower case as each letter is identified. If they guess what is written before you are finished then that's great – all part of code-breaking!

4) You can now tell the students how you wrote the message in secret writing in the first place. *You may wish to ask them what they think before you reveal the technique.*

    Say that to write a secret message you first write it in English in lower case letters. Then using the wheel, you look for each letter of your normal message ("plain text") on the outside wheel and write down the capital letter just inside it. *At this point, depending on the age/ability, you may wish to let the students try encrypting something. For more able students, this can wait one stage.*

5) It is worth mentioning that this system was developed by Julius Caesar who was a Roman Emperor. (A very powerful ruler who controlled much of Europe and Africa before Jesus was born.) It is worth having a chat about why people might want to write in secret.

    1. Of course, in Caesar's case, it was to avoid enemies – you can work through a scenario where enemies capture a message requesting more arrows to be sent – their likely response will be to attack.
    2. If one owned a bank, one might want to keep a secret of when the money was to be delivered, or where it was stored.
    3. One might wish to send a secret text message to a boy/girl without anyone being able to understand it. For example to ask someone to stop bothering you. *(This idea is fun and will get them giggling, but it's probably best not to encourage illicit relationships!)*
    4. See what other thoughts they have.

6) So, we have a way to write a secret message – but suppose you have one of these wheels and so does your friend, but someone finds the wheel. Can they read the messages now? *(yes!)*. Would the students like to see a better way to write a secret message? One that is more difficult to work out?

   Tell them they can do it with a computer you've built. Would they like to see it? Bring out one of the rotating discs (arrange it beforehand so that it is lined up like the previous disc). Explain that this is your encryption computer. Look at its features with the students.

   1. It has all the same features as the first one.
   2. But now the central disc can move. Get the students to work out how many positions it has. (26). Are they all useful? (No, in one position the letters line up with themselves and won't hide the plaintext.)
   3. Admit that it's not a very good computer!

   Describe how this new disk would be used. With one's friend, one agrees a letter to use as a "key" to "lock" the messages. Put the "A" on the inside disk next to this letter (for illustration, ask for a student volunteer to rotate the disc so that "A" on the inside is next to "Z" on the outside. Now one would use the disc in the same way as before. When you're finished, you put the "A"s next to one another and even if someone finds your disc, they won't know what position to use.

   Show the students the sheet marked "R13" for Rotation 13 in the top corner (the mark is for you, not the students so don't draw attention to it.) Tell them that it's written using this new code wheel but you're not going to tell them which position to put the wheels in. Remind them how to decode a message using the wheel and then ask if they're ready for a competition. (*hooray!*) Divide them into two teams (or three if there are enough discs and enough children). I used to do this by saying "all the clever students over by the tree and all the stupid ones by the grass". Once they'd all reacted (either by standing up or laughing) I'd tell them I was only joking and divide them up in some other way. Give one person in each team a wheel and check they have at least one notebook in each team. Ask them to pick a team name (to help build a sense of competitiveness.) Now let them start trying different positions on the code wheel to try to work out the message. *Depending on the situation, you might want to let one student, or one team, in on the short-cut. Alternatively let them work it out themselves and discuss it later. The shortcut is, of course, to identify that the one-letter word at the beginning could only be one of two things ('A' or 'I').*

7) Once one team has broken the code ("i love science") end the competition and declare them the winners. Get a round of applause. Now do some peer teaching – hopefully the winning team will have used the shortcut. Get the losing team to explain their method – you can use this to make a point about learning from each other. The winning team (if they found the shortcut) or you should now explain the shortcut method. Point out that both techniques are cryptanalysis. The first is a "brute-force" method – guaranteed to work, but slow. The second is more clever and faster, but not guaranteed to work. *One can look at how much faster it is. The students earlier identified that there were 26 positions for the wheels. (25 actually) However, if they use the shortcut then there are only two positions to try – this is an improvement of 12.5 times in speed.*

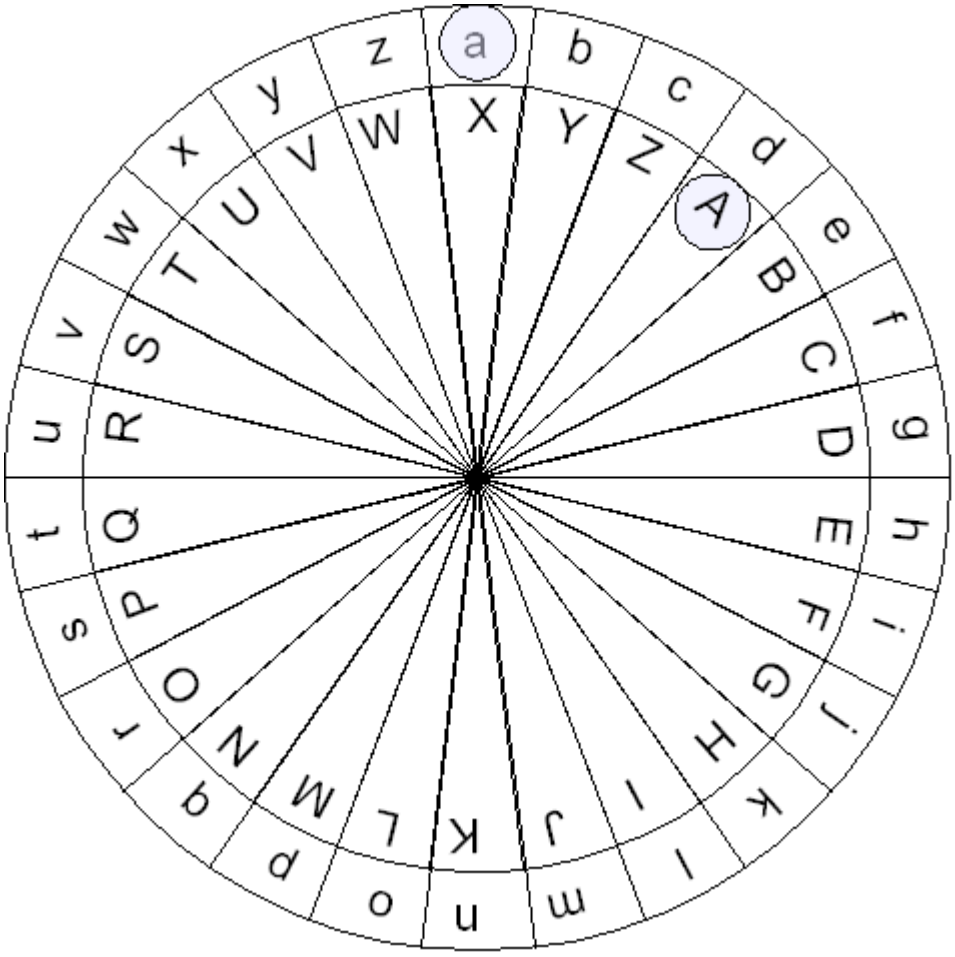
8) So, at this point, you may want to allow the students to try writing messages to each other depending on time and how they're doing. If they have moved quickly enough, one can discuss the security of different encryption methods. Ask the students to think about how much more secure the second code was than the first. Ask them if they think it is a good way to write a secret message. *In my experience they tend to say, "yes".* Point out that they were able to break the code in only a few minutes. Ask if it would be good enough for a bank, or government to use? They should identify that it's not very secure at all – though much better than the first code. The code they just did had 25 different "keys". You can show them (if there is time) a code which has more than 400 million million million million possible "keys". Do they want to see how to do that?

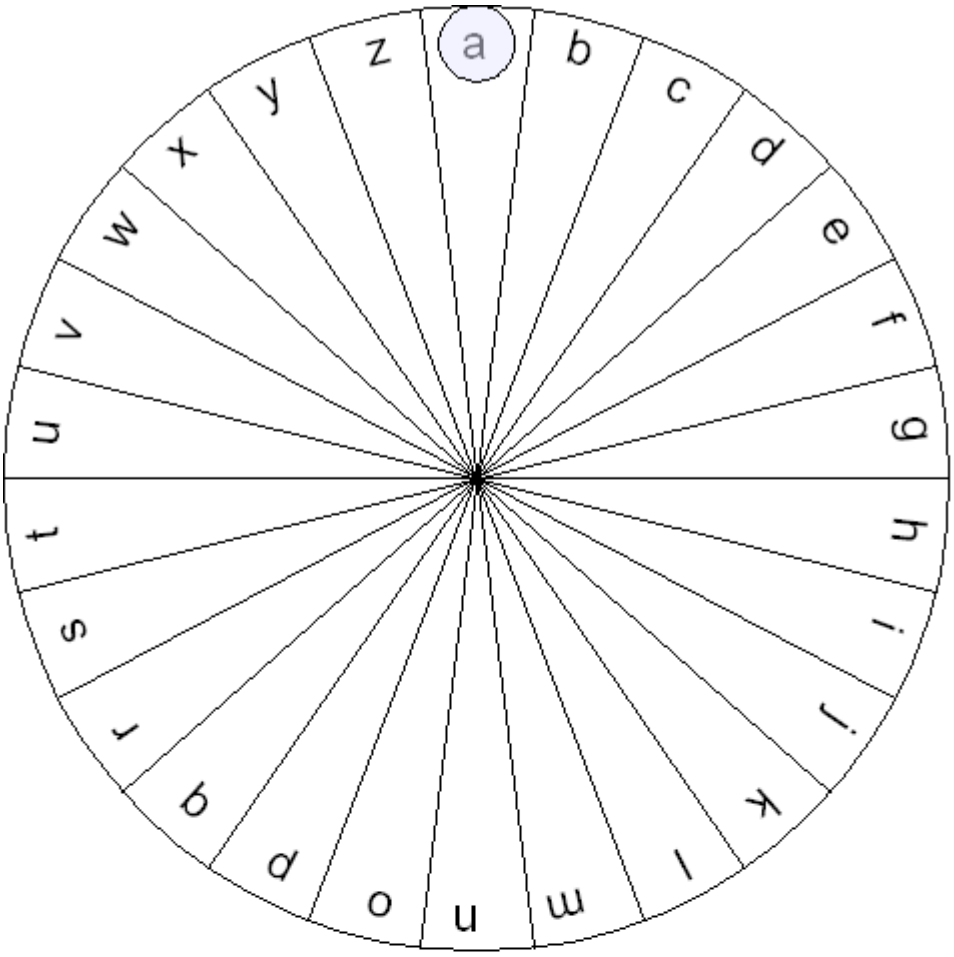
9) *Now you can use the incomplete key generator which has the alphabet in lower case written on it.* Remind the group that in the code they've just tried, the alphabet was just moved. This meant that as soon as one letter had been found, the task was over as all the other letters lined up. What about if instead of just moving the alphabet, you mixed it up completely? Show the students the key generator. Point out the lower case "plain text" alphabet. Say that instead of writing the alphabet in order but moved by some places, we are going to "randomize" the alphabet. So it might begin "p, y, o, e, c, ...". Discuss the difficulty of memorising this and the danger of writing it down. We will cheat – ask the students to name a favourite animal. Write it under the alphabet, in capital letters, missing out any repeated letters. Now ask for another animal and do the same, carrying on from where you left off. Now fill in the rest of the alphabet in order starting at the earliest letter which has not yet been used and missing out any other letters which have been taken. *(See the completed key generator for an example – in this case it was written with "Scientist" and "Farmer" as the two keywords.)* Now run over again how to encrypt from plain text to cipher text and vice versa. They should realise that in this code, if we find out which letter represents "I" it doesn't help us much.

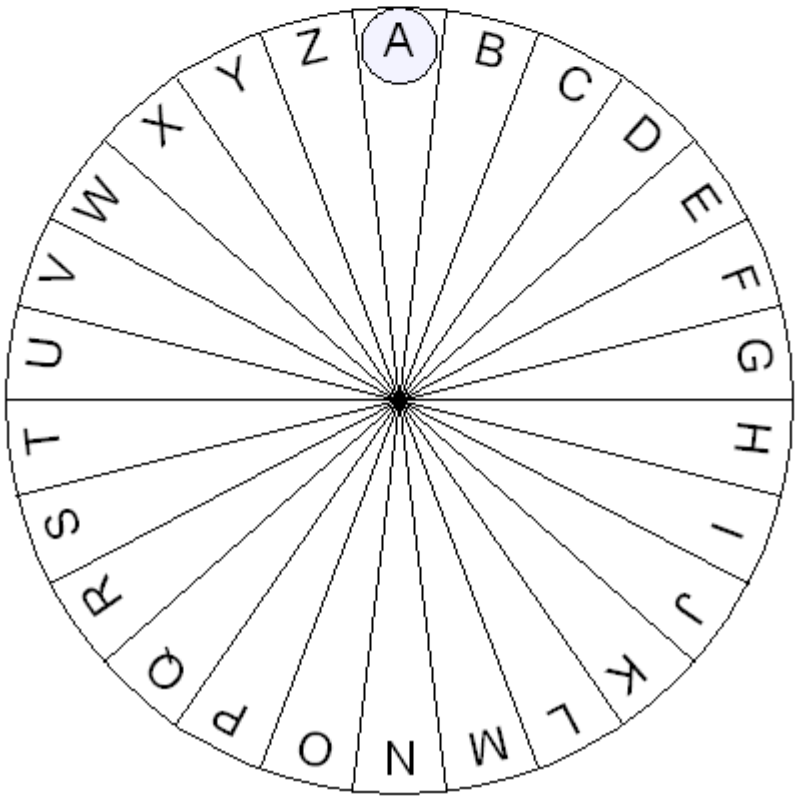
10) One can then move on to discuss random letter substitution and how it can be broken by frequency analysis (discovered by an Arab in about 900 AD). The largish body of text labelled "RS" is such a message generated using your own (also provided for reference) "key" Can the students uncover the message this time? If there is time, you can let them count the letter frequencies (show them the information on which letters are most common in English and discuss the logical process by which this information is useful.) Or just tell them that you have counted the letters and that N, Q and S were most common. Once these letters are added in (using a whiteboard marker on the plastic wallet holding the message, writing under the code messages in lower case) the students can start to guess at words and fill in the blanks to reveal "The Earth is my home. Everybody shares it with me. We must all protect the environment together."

11) Other areas for discussion can include modern encryption techniques; historical episodes in which encryption has been important (e.g. Mary Queen of Scots, Enigma); the Vignere cipher (which can also be performed using a code wheel) and how it remained unbroken for so many years; the one-time pad (unbreakable); quantum cryptography; the politics of law governing encryption.

12) To Close. It is worth discussing the purpose of your visit to their school/centre. Was it just to teach them how to write secret messages? No! It was to show them a different part of science that doesn't often get taught in school. It was to show them that science could be fun and useful. It was to show them that they can all do science. Is science something that you only have to know for school? No! Science is used everyday by all of us. Learning to think in a scientific way helps prepare us for life so that we can be better engineers, or doctors, or cooks, or cleaners. Thank the students for their time and encourage them to challenge each other with secret codes later.


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

C3

ZLPJLP / BARZXQFLK

R13

V / YBIR / FPVRAPR

abcdefghijklm plain

CIPHER

nopqrstuvwxyz plain

CIPHER

QAN NSOQA RP GY AJGN. NVNOYCJEY PASONP RQ WRQA GN. WN GUPQ SDD KOJQNIQ QAN NHVROJHGNHQ QJFNQANO.

RS

The most common letters in English are:

E, T, A, O, I, N

a b c d e f g h i j k l m	plain
S C I E N T F A R M B D G	CIPHER
n o p q r s t u v w x y z	plain
H J K L O P Q U V W X Y Z	CIPHER