University of Glasgow

QUANTUM TECHNOLOGY SCHOOL 20 21

ACADEMIC PACK

PART 1: CIPHERS: TEACHERS PACK

Dr Sarah Croke, School of Physics & Astronomy, University of Glasgow

Task 1.1: Caesar cipher

Q1 and Q2 a: suggested topics (feel free to use your own, or get the students to come up with their own):

TOPIC					
World leaders	Johnson	Modi	Macron	Trudeau	Putin
Famous scientists	Einstein	Curie	Newton	Hawking	Bell Burnell
Countries	China	Germany	Australia	Korea	Brazil
Cities in Scotland	Glasgow	Edinburgh	Aberdeen	Stirling	Inverness
Rivers in Scotland	Clyde	Kelvin	Annick	Dee	Don
Muppets	Kermit	Fozzie	Gonzo	Animal	Piggy
Star Trek ships	Enterprise	Discovery	Cerritos	Voyager	Defiant
Weasleys	Ron	Percy	Ginny	Fred	George

Q1 and Q2 b: The decrypted words are Doc, Sneezy, Bashful, Grumpy, Sleepy. These are all names of dwarves from Snow White and the Seven Dwarves.

Q3: The decrypted message is: Bob, meet me at eight – Alice, and the shift was +9 (so the students will need to shift *back* nine places in the alphabet to decrypt).

Q4: This was a good attempt at security in Caesar's time, when many people couldn't read, and those who could were perhaps not expecting messages to be encrypted: anything intercepted would look like gibberish. The students will have shown if they managed to decrypt Q3 that this is not really secure now however: just by searching through the 26 possible shifts, anyone can decrypt any message encoded in this way. Further, an eavesdropper only needs to try out all the possible shifts on the first few letters until they uncover a word that makes sense: this then gives the key which allows them to decrypt the rest of the message quickly.

Task 1.2: Variable shift cipher

1. The hangman game is intended to get students to think about the fact that different letters occur with different frequencies in the English language, and in addition some sequences of letters appear together more often than others.
2. This is not easy! And it's up to you how much time to give your students to keep working on this – past experience shows that students enjoy the puzzle, but once they get stuck into it they find it difficult to put aside and move onto the next exercise. You might want to encourage them to put it aside and think about it outside class. If they manage to decrypt the message, please post their solution here: https://forms.office.com/r/KMFj8338EH – you'll be asked to tell us the decrypted message and the name of your school. *Hint:* it is an historic quote, with a science and technology theme.
3. The puzzles should have shown that it was much harder to break the encryption in this case. In the first task an eavesdropper only needed to try (at most) 25 possible shifts before they find the one that works. For a variable cipher in principle the eavesdropper has to try every possible permutation of the alphabet – there are 26! of these (this is a *very* large number of possibilities). However, as discussed in exercise 1, in the English language (and indeed in other languages), different letters occur with different frequencies. If a message is encrypted with a variable shift cipher it is possible to try to break the cipher by looking for the letters which occur most often, making a guess for these, and piecing together the rest of the message –

students will probably have followed a strategy similar to this in tackling exercise 2. For a long enough message the number of occurrences of each letter is enough to completely break such a cipher: a variable shift cipher is not secure.

Task 1.3: One-time pad

1. Why is this more secure than the variable shift cipher discussed previously?

Solution: Because a different random shift is applied to each letter in the message, the encrypted message also appears completely random to someone who doesn't know the sequences of shifts applied. Compared to the variable shift cipher: in the variable shift cipher each letter of the alphabet is replaced by another fixed letter of the alphabet everywhere it occurs in the message, e.g. "a" is replaced by "b" in the example table given in task 1.2, "b" is replaced by "h", and so on. In the one time pad this is not the case – e.g. in the example in task 1.3 "A" is replaced by "D" the first time it appears in the message, but by "C" the second time it appears. The output string of letters appears to be random, and we can no longer learn anything by looking at how frequently different letters appear in the cipher text.

2. What is the key in this case?

Solution: The "key" is the sequence of shifts applied: 17, 13, 2, etc: anyone who knows these can easily decode the message.

3. Do you think this encryption method is secure? Why/why not?

Solution: This is for discussion, to see what the students think. As long as the key is random, and is kept private and known only to sender and receiver, this is provably secure against any attack, even by an eavesdropper with unlimited computational power.

University of Glasgow

Binary digits:

Exercise:

1. Assuming your mobile phone operating system uses ASCII encoding, how is the name Bob stored in binary by your phone?

Looking up the table gives:

B 01000010

O 01001111

B 01000010

So Bob is stored as 010000100100111101000010. (Also possible to use lower case).

Exercises:

1. In the example above, anyone who has the key should be able to decode the message. How would you do this?

   Solution: Given the cipher and the key, encoding is the same as decoding – if the key has a "1" in a given position, flip the cipher bit in that position to obtain the plaintext bit.

2. Below is an example of a sequence of three ASCII characters that have been encrypted using a one-time pad. The key is given – can you find the characters?

Cipher	1	0	0	1	1	1	0	0		0	1	1	1	0	1	1	1
Key	1	0	1	0	0	1	1	0		0	1	0	1	1	0	1	0
Plain	0	0	1	1	1	0	1	0		0	0	1	0	1	1	0	1

Cipher	0	1	1	1	0	1	0	0
Key	0	1	0	1	1	1	0	1
Plain	0	0	1	0	1	0	0	1

Characters: The characters are : -)