STEM LEARNING

NUMBER 1 FOR STEM

Quantum Technology

PROGRAMME

TEACHER GUIDANCE

Quantum encryption keys

1 BACKGROUND

The need for more secure encryption

Quantum computers are set to become operational in the very near future. These innovative machines will be capable of specialised computation vastly superior to any ordinary computers. The security of conventional methods of encryption based on the RSA (Rivest–Shamir–Adleman) public-key cryptosystem could become obsolete and exposed to cyberattacks with the advent of quantum computers. Networked Quantum Information Technologies (NQIT), part of the Quantum Technology Hubs, is developing the Q20:20 quantum engine. This is a network of 20 quantum processors (each containing 20 matter q-bits) that share information via photons. This highly complex and powerful design will put the UK at the very forefront of quantum computing.

The Quantum Technology Hubs are also developing more secure ways to share encryption keys based on a protocol called BB84. Watch this video to see how the Quantum Technology Hubs are developing safe ways to share encryption keys and to understand how eavesdroppers could be detected.

In this activity students will carry out a few decryption tasks and develop an understanding of the importance of keeping messages secure from hackers and other criminals. Finally, students will understand the basics of how RSA public key distribution works and why quantum key distribution is becoming necessary with the development of quantum computers that could crack the RSA key distribution protocol in a matter of minutes.

2 OBJECTIVES

- Understand the basic principles of how messages are decrypted in digital communications
- Describe in simple terms how RSA key distribution works
- Explain why quantum key distribution is becoming essential in digital communications

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

3 ADVANCED PREPARATION

- A projector, speakers and access to YouTube would be useful.
- We recommend reading the teacher information carefully before carrying out this activity. There are some cards and messages to the students that need to be prepared in advance.
- Download the PowerPoint presentation to support the 'Quantum Key Distribution' activity in the activity sheet.
- Three polaroid filters and a light box/small torch could be used to demonstrate the BB84 protocol (see PowerPoint 'Quantum key distribution and entanglement').

4 INTRODUCTION

In this activity students will need to decode a simple message that will give them access to a key needed to decipher a second message. This first activity simulates a communication sequence between a sender and a receiver. They will then work through a simple demonstration to gain an appreciation of the practical difficulty of finding the two prime numbers that are sent as their product in RSA keys.

Finally, quantum key distribution will be explored as a secure means for sending encoded messages following the imminent quantum-computing revolution.

5 ACTIVITIES

The activity sheet contains a set of tasks for the students to develop their understanding of conventional encryption methods and emerging quantum key distribution.

6 PLENARY

The implications of developing networks that can share encryption keys using quantum key distribution are quite significant. For example, a whole new infrastructure would need to be built to achieve this on a large scale. Students could be asked to discuss the following questions as a plenary to this activity.

- Compare and contrast the RSA methods for encryption key distribution with quantum key distribution
- What will be the advantages of using quantum key distribution over traditional encryption key distribution?
- What are the disadvantages of using quantum key distribution?
- What innovations do you think will be needed to make quantum key distribution commercially viable and accessible to a large number of users?
- How would you find out about how to pursue a career in this field?

7 EXTENSION

This activity is already quite rich and it will require some time for the students to complete, but we have suggested additional resources and links in the 'Links to further resources' section.

8 TEACHER INFORMATION

In the encryption part of this activity we took much inspiration from this resource from the Royal Institution.

In the first part of the activity students will need to decipher a simple message using a 'shift cipher'. You should print small cards for each student with the message: "The letters in the message have been shifted, find the solution to obtain the key". But to one student only (or group, if they are working in small groups) you should give them the card with the correct 'shift cipher', ie "The letters in the message have been shifted by five places forward in the English alphabet. Use this information to decode the message and obtain the key".

The students should be told not to share their messages with anyone else and show the decoded message to the teacher and no one else once they've cracked it. We would suggest not to tell the students that one student has the correct cipher, but later in the activity (when the students will approach the demonstration with prime numbers) the teacher can explain that the person/group who had the 'shift cipher' was the intended recipient and could work out the coded message to obtain the key pretty quickly, whilst the others were hackers trying to tap into the communication channel.

At this point it would be useful to explain that RSA public key distribution is virtually impossible to crack with ordinary computers because the factors of two very large prime numbers multiplied together would take several thousand years to compute, even with the most powerful computer. The complexity of calculating these two prime factors is the reason RSA encryption key distribution is currently a fairly secure method of sharing secret information. However, with quantum computers these computations would be trivial and an RSA key would be cracked within minutes by a quantum computer. Therefore, the students who didn't have the key, but who managed to decipher the first message by working out the shift cipher, could be compared to quantum computers (they will like that). It is important to stress that RSA public key distribution is not a 'shift cipher' and it is much more difficult to crack, but the time it should take students to work out the shift in the alphabet is a good analogy for a quantum computer cracking an RSA key. Also, the fact that every student knew the method of the cipher (ie that the letters were shifted) is akin to the RSA public key method, as two prime numbers are shared publicly as (Prime Number 1) x (Prime Number 2).

The encoded message is VZFSYZR UMDXNHX NX FBJXTRJ.

The letters in the alphabet are shifted by five spaces forward, so the 'shift cipher' looks like:

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
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

And its shifted decoded message reads QUANTUM PHYSICS IS AWESOME.

If some students really get stuck, it could be suggested to them that the last word has two letter 'E's in it.

How do we use encryption keys?

When a student gives you the correct message you should share the key with them as a small card with the sentence: "The first eight letters of the name ALBERT EINSTEIN are the key to decode my message".

The students should write in their worksheets the letters in the eight boxes provided, as below:

A	L	B	E	R	T	E	I

The students should then convert their key to a binary key. In their worksheet they will be told that the conversion of the key follows the rules:

1) Every vowel becomes a 1
2) Every consonant becomes a 0

So, the binary key will be

1	0	0	1	0	0	1	1

The students should now apply a XOR operation for each character in their encoded binary message to decode the message by looking up the binary letters in the ASCII grid provided.

The XOR operation can be summarised as:

0 0 = 0

0 1 = 1

1 0 = 1

1 1 = 0

So, if an 8-bit binary code is received as 11001010 the students would need to match each digit with the corresponding digit from the key above and change the 8-bit binary code using the result from the XOR operation, as shown below. You could share this table with your students to help them understand this process.

Encrypted binary code	1	1	0	0	1	0	1	0
Binary Key	1	0	0	1	0	0	1	1
Decrypted binary code after applying XOR operation	0	1	0	1	1	0	0	1

At this point the students will need to apply the XOR operation to the encoded binary message in their worksheets. If they apply the rule correctly and if they can convert all the binary letters into letters of the alphabet they should get the following message.

Encoded binary message:

11000010 11000111 11010010 11011101 11000111 11000111 11011110

11010000 11010110 11001010

11010111 11011010 11000000 11000111 11000001 11011010 11010001 11000111 11000111 11011010 11011100 11011101

Decoded binary message:

01010001 01010101 01000001 01001110 01010100 01010101 01001101

01001011 01000101 01011001

01000100 01001001 01010011 01010100 01010010 01001001 01000010 01010101 01010100 01001001 01001111 01001110

Binary letters converted to alphabet characters: QUANTUM KEY DISTRIBUTION

Public key cryptography

In this activity we propose a simple role play where the students will be given the public key number n, which is the product of two 3-digit prime numbers, p and q. Each student has a 3-digit prime number next to their name (you will need to fill in the table in their worksheet before the start of the lesson with their names – see example below).

Alex	263	Delyth	241	Kyle	409	Mollie	311
Alice	373	Dalia	227	Kylie	257	Nadia	449
Awel	379	Elisa	313	Laura	347	Noah	479
Bob	353	Elsa	389	Leah	281	Norah	509
Brin	397	Emmanuel	349	Lyon	307	Ollie	331
Callum	283	Francis	457	Luca	421	Paul	439
Cassandra	463	Fred	251	Martin	317	Pete	503
Colin	499	Gabriel	467	Marcus	461	Sarah	233
Connor	443	Gaby	359	Mark	293		
Debbie	491	Ken	401	Megan	223		

Next, choose one of the student's prime numbers without revealing your choice to anyone and multiply it by 229 (another prime number). For example, if your receiver is Gabriel (467), n = pq = 229 x 467 = 106,943.

Now send n publicly out to all students and ask them to divide n by their own prime number. If they are the receiver they will be the only one able to obtain an integer (prime) number (p = 229), if not they will have to try all other prime numbers to see which one obtains an integer prime number.

You will need to warn that the receiver should not reveal they are the intended recipient of the message, or the game will be spoiled.

After this activity you should explain to the students that:

- p and q are chosen by the receiver
- the receiver sends n (the product of p x q) to the sender
- the sender uses n to encode the message
- the receiver uses p and q to decode the message and read it

RSA cryptography is more complex than this, and more information can be found here (for students who might be interested in finding out more), but the steps above introduce the students to the idea of public keys that can support their understanding of the need for quantum key distribution.

The idea of public keys can also be demonstrated using a phone book – any number can be found from a given name very quickly, but a name cannot quickly be found from a given number. It is do-able, but only slowly – just like public key encryption.

Quantum key distribution

Below we have suggested some possible answers to the questions from this simulation https://goo.gl/X4xXTF as a guidance. A PowerPoint presentation is available to help you introduce the activity and the principles of quantum entanglement and quantum key distribution to your students. Two videos are also suggested on the students' activity sheet if they want to develop their understanding further.

1) Why does Bob need to invert the values of the outcomes measured along the same orientations as Alice to produce his key?

   Because, for any measurement obtained along the same orientation, the particles measured by Bob will have the opposite spin to the particles measured by Alice. This is because they are entangled and measuring the spin of one automatically determines the spin of the entangled particle along the same orientation (no matter where it is).

2) Activate all display controls, set the orientation of the SGA devices to 'Random orientations' and allow Eve to intercept and resend particles by clicking on the button 'Eavesdrop!'. Click on 'Fast forward 100 particle pairs' and click on 'Let Alice & Bob compare 20 bits for errors'. Make a note of the number of errors found and repeat a few times. What did you notice? Can you explain why this happens?

   Because this is a random process.

3) Why isn't Eve able to resend a particle to Bob always with the correct spin?

   Because Eve doesn't know which orientation Alice has used for each particle until both Bob and Alice have shared the orientation for each spin measurement, but Bob needs to have received the particle re-sent by Eve before he will make that information public.

4) Why is it important that Alice and Bob measure each particle independently of each other and choose random orientations?

   The process needs to be completely randomised. If any pattern in the choice of orientation is predetermined, it could be spotted and an eavesdropper could match Alice's orientations and always send a particle with the correct spin to Bob, hence hack the communications.

5) Explain why quantum entanglement ensures the key is shared securely between Alice and Bob.

   Once the orientations of each spin measurement are known, Bob and Alice can discard the measurements along different orientations and keep the ones along the same orientation, because they will be opposite spin, due to the quantum entanglement of the particle pairs. However, if a hacker has intercepted the particles and re-sent particles to Bob with random spin, Bob and Alice will know that someone has disturbed their measurements. In fact, Bob will measure some particles along the same orientations measured by Alice that have the same spin as Alice's particles. This is not possible for quantum entangled particles, so they will know that someone has interfered with their measurements and can discard the key they generated.

9 LINKS TO FURTHER RESOURCES

Your students could watch this video to understand the basic principles around quantum key distribution and you could explain this animation after the video is shown to help them understand how eavesdroppers can be detected. Alternatively, students could watch the video above before the lesson.

Interesting resources that could be used as extensions to this activity are listed below:

- https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/BB84_photons/BB84_photons.html
- https://nrich.maths.org/2200
- https://nrich.maths.org/2199
- https://nrich.maths.org/7940
- http://www.maths.manchester.ac.uk/cryptography_competition/
- https://www.stem.org.uk/resources/elibrary/resource/32314/lorenz-cipher-machine
- https://www.youtube.com/watch?v=mthPiiCS24A&feature=em-uploademail