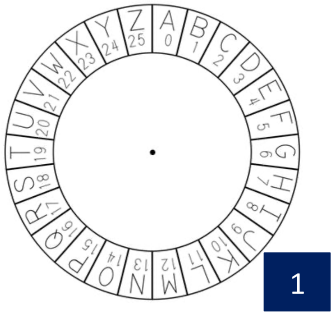
Cryptology, A Tango of Increasing Difficulty.

> *I have never done anything "useful". No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world.*
>
> *- G. H. Hardy, a pure mathematician, who enjoyed tangoing with number theory*

Perhaps for most people, numbers are just for arithmetic, besides that, why care?

Caesar's ring



1

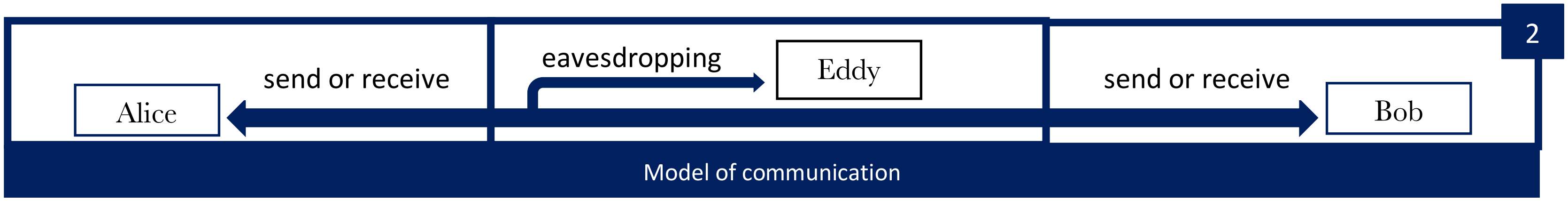
2000 years ago, Julius Caesar noticed the importance of security in military communications, so he encoded his messages by shifting each letter by a certain amount. For example, Caesar's last words in **plaintext**: "You too, Brutus?", all shifted by 8 would become the **cipher**: "Gwc bww, Jzcbca?", making it incomprehensible to anyone else.

Such a system is known as a **symmetric cryptosystem**, as the receiver and sender both have the same information regarding the encryption. Namely, both of them can encrypt and decrypt messages. In this case, Caesar (sender) and his general (receiver) would both have known the secret of shifting by 8 letters according to Caesar's ring (figure 1). Such crucial information that's kept secret to decode the message is known as a **private key**, while other public information is called a public key.

However, a person could, by trying at most all the 25 possible "shifting values", crack Caesar's cipher using only pen and paper. Generally, there are other problems for Symmetric encryptions. As, Caesar would need to meet each person on his contact list and agree on a unique shifting value. What if he wants to speak securely to millions through a social media?

Cryptology has evolved since Caesar's time. After World War 2, the decryption work done on Enigma (a diligent symmetric cryptography machine) brought more confidence in using machines to process information rather than just human brains. The use of Computers to crack code, rapidly became common due to their promising calculational power. Old encryptions became vulnerable.

Therefore, in 1976, Diffie and Hellman introduced the general concept of **asymmetric encryption**. It allows encryptions taking place without a first meeting. Instead, a one-way trapdoor encryption is used in most asymmetric systems, so that only the receiver can easily decrypt the message. Diffie and Hellman have also published a specific asymmetric encryption protocol called the **Diffie-Hellman Key Exchange**. This method helps the sender and the receiver to agree on a private key from distance in secret, for the use in future encrypted communications.



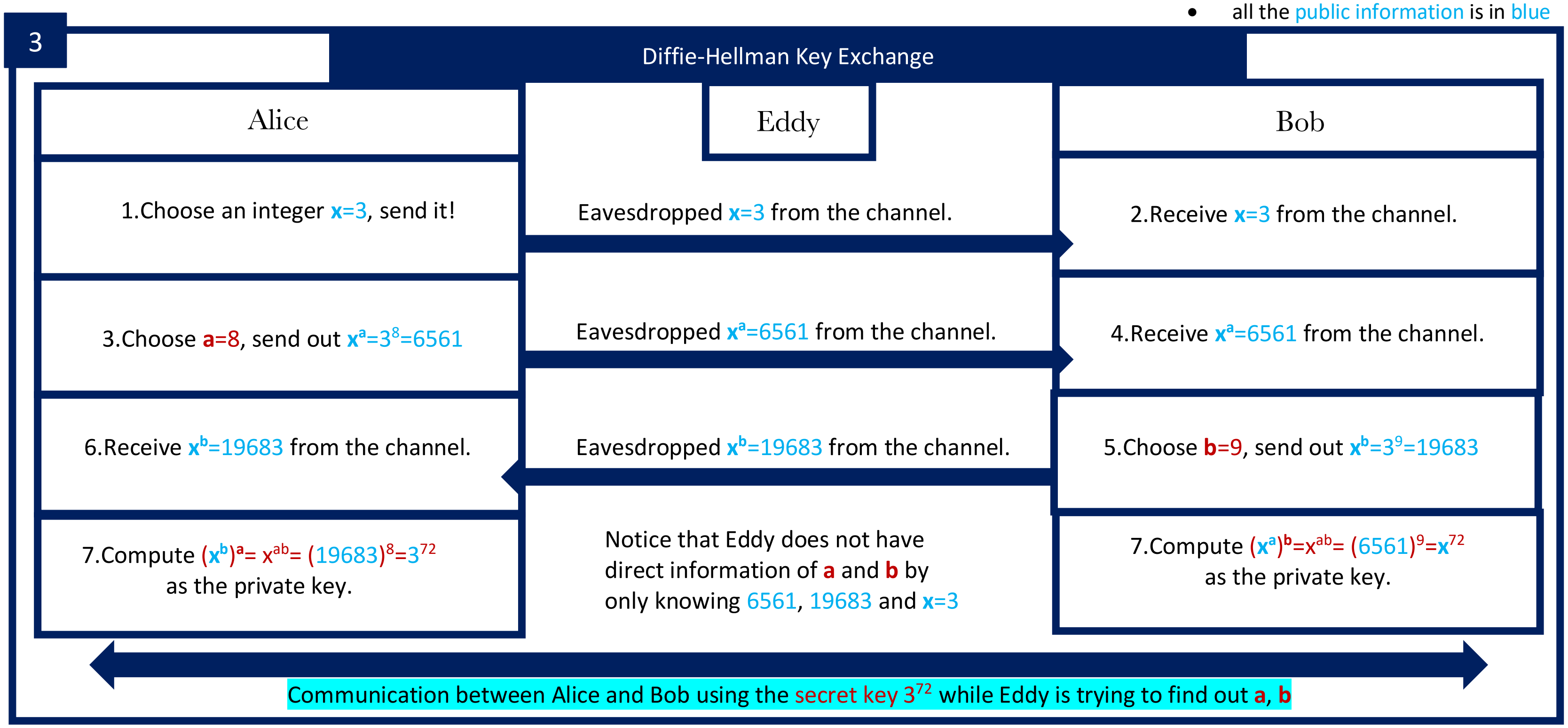
2

Model of communication

A **cryptography model** (figure 2) usually involves three fellows: **Alice, the sender**; **Bob, the receiver**; and **Eddy, the eavesdropper** who can hear anything in the communication channel (These names will be used later). Encryptions are needed so that Eddy would not be able to understand the message that's passing through the channel.

Figure 3 demonstrates how Diffie-Hellman Key Exchange operates on integer multiplication.

- all the private information is in red
- all the public information is in blue



3

Diffie-Hellman Key Exchange

Alice

1.Choose an integer $x=3$, send it!

3.Choose $a=8$, send out $x^a=3^8=6561$

6.Receive $x^b=19683$ from the channel.

7.Compute $(x^b)^a= x^{ab}= (19683)^8=3^{72}$ as the private key.

Eddy

Eavesdropped $x=3$ from the channel.

Eavesdropped $x^a=6561$ from the channel.

Eavesdropped $x^b=19683$ from the channel.

Notice that Eddy does not have direct information of **a** and **b** by only knowing 6561, 19683 and $x=3$

Bob

2.Receive $x=3$ from the channel.

4.Receive $x^a=6561$ from the channel.

5.Choose $b=9$, send out $x^b=3^9=19683$

7.Compute $(x^a)^b=x^{ab}= (6561)^9=x^{72}$ as the private key.

Communication between Alice and Bob using the secret key 3^{72} while Eddy is trying to find out **a**, **b**

Even without knowing **a**, Bob can get the same private key as Alice (3^{72}), since $(x^a)^b=(x^b)^a$ and Bob knows x^a and **b**. Yet for Eddy to find the private key, he would have to try all the possible values for a and b, so more computation is needed compare to Bob and Alice who just need to do multiplication. If instead of using integer multiplication, Alice and Bob operates on other algebraic systems (more precisely, cyclic groups), then even more computational power could be required for Eddy to crack the system.

The most effective asymmetric encryptions are formed based on unsolved maths problems, and by choosing the right question, an asymmetric cryptosystem can be constructed to encrypt all messages (rather than just exchanging a private key and carrying on with a symmetric system).

Rivest, Shamir and Adleman (right, middle, left)

One of the most well-known asymmetric cryptosystems is based on the difficulty of **prime factorization**. It is known as the **RSA-cryptosystem**, constructed by **R**ivest, **S**hamir, **A**dleman in 1977. It relies on the fact that, multiplying two large primes can be done easily by a computer, but factorizing the product to find the two primes would require trying all the combination of known primes. Give it a try, 3983779423213 (Product of 1998949 and 1992937) is a product of two primes, can you factorize it quickly? Now imagine a product of primes with digits so long that I will 'exceed' my word limit if I put it here. Up to today, an efficient way of factorizing primes has yet to be found.

How RSA is related to prime factorization

Using RSA, Bob as the receiver will decide a value **n** **as product of two large primes p and q**, such **n** will become part of the encryption and will be broadcast, so Alice can use this encryption to encrypt the numerical form of messages and send the cipher to Bob. However, the only mathematical way to find the inverse will require using the value of primes **p** and **q**, which is only known by Bob, hence Bob can easily reverse the encryption and obtain the plaintext. If Eddy ever wants to know the plaintext, he will have to factorize **n** to find out **p** and **q** and then decrypt the cipher, which is yet still very hopelessly hard to complete in short term.

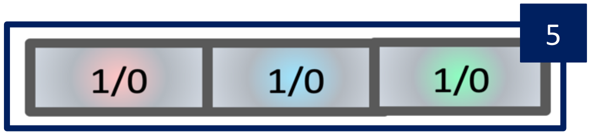
RSA is so strong that even today, super computers are powerless when cracking it. Because of this, RSA was chosen to be an essential part of the Hypertext Transfer Protocol Secure (https), the communication protocol of the internet, that allows private information to be transmitted securely. Gauss (a genius mathematician) actually spent years of his life working on quick factorization but only made a little headway. It's not yet proven that there is no way to obtain private key **p** and **q** from public key **n**, but it is true that it has withstood decades of attacks and none have succeeded. Because of RSA, mathematics has found another application, turning methods of prime generation and factorization from curious wonders into assets of security. When primes where first examined, it must be astonishing for the Greeks that these numbers would someday become an essential element underlies information security, that secret agencies are willing to develop better methods and machines to tackle problems that G H Hardy loved as they are "useless".

All these complex encryptions were built up using logical thinking based on experience in numbers and other fields of maths. But while mathematics and traditional computer thrives, the discoveries in quantum physics brought a new aspect to modern computation methods. Soon, new types of machines will rise, and outrun the cryptosystems that we rely heavily on today.

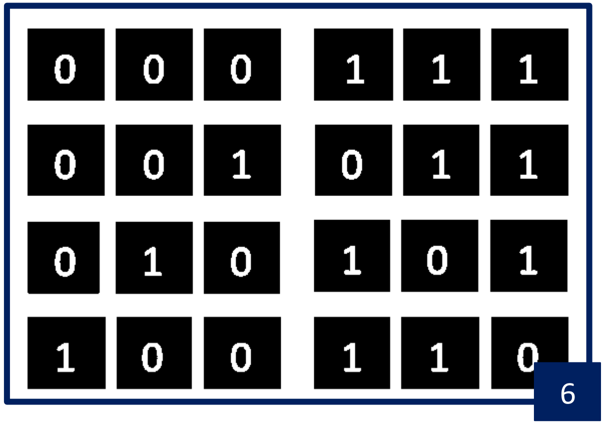
Theoretically, a quantum computers can manipulate different sets of data simultaneously by the superposition of 'tiny' particles, running exponentially faster than traditional computers. Instead of trying each combination of primes, a quantum computer can have almost all the combinations processed at once. The difficulties in solving prime factorization will no longer exist. Making current systems vulnerable. Hardy's hard and "useless' questions are once again needed.

One candidate cryptosystem is Lattice based cryptosystem. A lattice is a set of points that can be formed by scaling given vectors; forming a field of points. Questions concerning relationships among these points can perhaps be very difficult, even for quantum computers. Making it a competitive candidate for quantum age.

3 bits can be written into different binary sequence, but 3 quantum bits can be all of them at once, as each quantum bit is a superposition of 1 and 0 . (Figure 5 shows 3 qubits, and Figure 6 shows 8 bits . we can see that 3 qubits can do the job of 8 bits of a traditional computer . In fact, by thinking of permutation, n qubit can worth 2^n bits .)



5



6

So far, all the quantum computers we have made are still extremely fragile to changes in their environments. However, just in case quantum computers manage to leave the lab someday, preparation is necessary. From the development of cryptography, we can notice the value of questioning, and how raising the right difficult question can be beneficial. The tango between encryption and decryption is a dance of ever-growing difficulty, the better a solver you are the harder the problem gets.

And how fortunate we are, to be part of this tango.

Reference:

(Figure 1) Caesar's Ring image source

(Figure 4) The photo of Rivest, Shamir and Adleman

(Figure 2,3,5,6 is made by me using Word)

History of Cryptography from SANS Institute

Diffie-Hellman key exchange reference

Public key history and RSA-cryptosystem reference

My source of quantum computing

Kurzgesagt video: Quantum Computers Explained – Limits of Human Technology

Video about RSA cryptography explaining step by step in detail

For more about RSA, this textbook covers all the foundations and a topic specified on RSA (page 280)

Video about Lattice based cryptosystem

The End.