classical cryptography:

* secret key/symmetric
  + one singular key, for both encrypting and decrypting the message. This means the sender and recipient must have the same key available to them.
  + Person A must physically share the key (through text, email, etc) with Person B before sending secure messages
  + Problem: don’t know if the key has been stolen by someone & messages could be intercepted.
* public/asymmetric key/RSA (the standard cryptographic algorithm on the Internet)
  + Person A sends an encrypted message to Person B using their public key (public key is known by everyone). Person B unlocks the message using a private key.
    - So message is encrypted with public key but decrypted with private key
    - How can a secret message be sent using public info?

<https://www.youtube.com/watch?v=UiJiXNEm-Go>

Encryption: so important, seen as a weapon regulated for national security, now ruled as free speech

Simple substitution: swap out each letter by a certain amount

More complicated encryption uses complex math - using one-way functions (RSA)

Similar to RSA (factorization of a large number into primes):

Using really large prime numbers and multiplying them together (p-1)(q-1)

Substitute letters in message for bits, conversion key from numbers to letters is *publicly* known

Multiply each of the numbers by (p-1)(q-1). Without knowing the factor is (p-1)(q-1), it would take hundreds of years to crack the code if you wanted to intercept the message since the private key is such a large unfactorable number.

You can use the public key to encode a message, but to decode it you need the prime factors, which only the recipient of the message has.

However, since quantum computers can speed up computation, RSA may not be a secure way to hide information.

Quantum cryptography (instead of math, relies on the laws of physics):

Making a random key

Step 1: Alice sends polarized photons (vibrating in four diff directions, 0- vertical & diagonal right, 1- horizontal & diagonal left)

Step 2: Bob the receiver randomly guesses which bases Alice may have used, translating photons into bits - 1 or 0. Bob measures the signal he receives from Alice.

Step 3: Now, Bob compares with Alice through a public channel. Alice chose a vertical base and got 0 bit, but Bob chose a diagonal base. He has a 50% chance of choosing bit 0 (diag right) and 50% of choosing bit 1 (diag left).

Step 4: Alice and Bob disregard bits with a different basis (even if they were the same bit). This results in a sifted key. Now, they have a key made out of the ones that matched up correctly.

Step 5: If Eve tries to eavesdrop, when Bob and Alice measure using the sifted key, usually 36+ bits there’s a 99% chance that Eve will have made a mistake and chosen a different base than Bob, leading to different results that don’t match up with Alice.

Power - eavesdropper needs to measure in order to get the key but when measured the key changes, you can know if you’ve been hacked even before you’ve sent the message

If you make a truly random key, you can theoretically make a code called a one-time pad that is unbreakable.

<https://www.youtube.com/watch?v=fLJ9mvTS68Y>

* Cryptographic codes used online are public key systems
* Public key means everyone knows how to encrypt the message but no one knows how to decrypt it
  + To encode the message, you use a method that is easy to do but hard to undo
* Post-quantum cryptography: cannot be broken even with quantum computers
* Quantum key distribution: method for two parties to securely share a key that they can use to encode messages
* Calls polarization spin
* If Eve measures in the wrong direction, she changes the spin of the particle. Bob notices his measurement result no longer is correlated with Alice’s (because once something is measured, it stays in that state forever). It’s impossible to copy an arbitrary state without destroying it - no-cloning theorem

<https://www.youtube.com/watch?v=4KCDGa98Ckc>

Shor’s algorithm: can factor multiplication of two primes way faster than a normal computer (less than a day)

Post-quantum/quantum resistant cryptography: might replace the more vulnerable prime factoring based cryptography

<https://www.plixer.com/blog/quantum-cryptography-explained/>

Quantum cryptography takes advantage of the properties of quantum physics to encrypt information at the physical network layer. Post-quantum and quantum-resistant cryptography efforts, however, remain focused on developing encryption methods that rely on hard math problems—the kind that quantum computing is not well-suited to solve.

Heisenberg uncertainty principle:

-the only way Eve can measure a photon’s spin is by passing it through a filter. If Eve measures the photon with a filter in the wrong direction, the photon’s spin will be altered & she will incorrectly read it. Unless she knows which filter to use, she’ll get it wrong about half the time.

How to stop Eve from eavesdropping? After Alice sends the key, she calls Bob and tells him which scheme she used for each photon (leave out the spin or whether it was 1 or 0), just whether it was rectilinear or diagonal. Same filter, keep digit, wrong filter, get rid of it. This won’t help Eve even if she’s listening in.

Why? Example: Alice - rectilinear, Eve - diagonal, Bob - rectilinear. Alice and Bob keep it, Eve used the wrong filter and can’t tell if it’s a 1 or 0 from which scheme they used. Example 2: Alice - diagonal, Eve - diagonal, Bob - rectilinear. Alice and Bob get rid of this answer but Eve keeps this. Eavesdropper cannot compare their results with Alice, but they would also change the photon positions that Alice and Bob expect to see.

Particles can exist in more than one place or state at a time

A quantum property cannot be observed without changing it or disturbing it

Whole particles cannot be copied