**Slide 1:**

Good Evening everyone, this is Neil Gupte and this is Aditya Kulkarni and today we will be presenting our topic for today which is **Shors Algorithm Basics and Implementation in Qiskit .**

**Slide 2:**

Lets start with understanding cryptography, I know we have covered it in class as well but just to give an brief idea we will go through it again. In essence it is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It ensures secure communication.

**Slide 3:**

So there are essentially two types of encryption used 1)symmetric and 2)asymmetric encryption.

Symmetric encryption is the simplest kind of encryption that involves only one secret key to cipher and decipher information. The sender Alice encrypts the plain text using the secret key and produces the cipher text. This cipher text is decrypted by Bob using the same key and receives the original message.

The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256,Blowfish.

**Slide 4:**

Asymmetrical encryption is also known as public key cryptography, Asymmetric encryption uses two keys to encrypt a plain text. A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Asymmetric key has a far better power in ensuring the security of information transmitted during communication. Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes EIGamal, RSA, DSA.

**Slide 5:**

Guys can anyone of you tell who these 3 gentlemen are ?

**Slide 6:**

Yes they are ron rivest ,adi shamir and leonard adleman who filed the patent for RSA algorithm for encryption in 1977 while being a faculty at MIT. They were given the A.M turing award in 2002 which is considered like a Nobel Prize for computing for their contributions to public key cryptography.

In the RSA system a user secretly chooses a pair of prime numbers p and q so large that factoring the product n = pq is well beyond projected computing capabilities for the lifetime of the ciphers.

If you can build a computer using ever electron in the universe as computational bit it would take that computer longer than the lifetime of the universe to decrypt a 3000 bit key. So we can assume that RSA keys are safe from attack from classical computers.

**Slide 7:**

This is a quote from the famous Max Planck a German theoretical physicist who originated quantum theory, which won him the Nobel Prize for Physics in 1918.

With the invention of quantum computers, we are expanding the computational capabilities of humans and are closer to solving the impossible.

**Slide 8:**

Can you guess who this person is ?

**Slide 9:**

This is none other than Peter Shor, who in 1994 developed a quantum algorithm for integer factorization, while working at Bell Labs in Murray Hill, New Jersey.

**Slide 10:**

This algorithm is now known as Shor’s Algorithm. The algorithm is significant because it implies that public key cryptography might be easily broken, given a sufficiently large quantum computer.

**Slide 11:**

These are the simplified steps in the shors algorithm. There is lot of modular arithmetic and linear algebra involved within each step, but we are not delving in deep into the actual mathematics.

But you must wonder where is the magic in all this?

**Slide 12:**

**Slide 13:**

Lets go over the steps by taking a trivial example of 15.

First we find take a random number lets take 4.

As the gcd of 4 and 15 is 1 we can continue.

Then we find the period of 4^x mod15 which comes out to be 2 which is even.

**Slide 14:**

**Slide 15:**

The quantum fourier transform helps us in finding the period of the function in polynomial time and is the main reason which enhances the computational time of shors algorithm.

**Slide 16:**

You guys might have heard about fourier transform in DSP where they basically they take in audio signal as a wave and convert it into a graph showing different frequencies that the wave is made up of.

**Slide 17:**

We should keep in mind that there is the repeating property to the period of the function.

If we take another power and add or subtract p to it then the amount more than our multiple of N stays the same.

This is important as QFT uses this property.

**Slide 18:**

Suppose we take superpositions of all possible powers in quantum computer and just measure the amount more than multiple of N part. Then we will randomly get one of the possible amounts more than a multiple of N as the output. That means we must be left with a superposition of purely the powers that could have resulted in the remainder of 3. Because of the repeating property all these numbers are p apart from each other.

**Slide 19:**

If you input a single number into the quantum fourier transform it will give you superposition of all other numbers ,where the superposition is weighted by different amounts and those weights look roughly like a sine wave.

If we put a higher number we get sine wave with higher frequency.

The important thing is if we put in superpositions of number then the output of QFT is superposition of of superpositions that is the sine waves add or cancel out .

**Slide 20:**

If we put superpositions of numbers separated by amount p all the sine waves interfere and the result is a single quantum state of 1/p as all the rest destructively interfere. Thus after finding the reciprocal of 1/p we get the p.

And that is shors algorithm in a nutshell. Although the underlying concept is pretty complex the core structure of the algorithm is very simple.

**Slide 21:**

The question arises, is rsa dead?

Thus as of now rsa is not compromised and our data is safe, But not for long.

Considering the extensive research and funding which is taking place in the field of quantum computing we would have build a big enough quantum computer by the end of next decade.

Many organizations have already started preparing for this by using post quantum cryptographic algorithms mainly BB84.

**Slide 22:**

So now we have come to the end of the presentation and now we will show the demonstration of shors algorithm in qiskit.