ECC Cryptography

Team Details

Sunny Kumar Pandit CSE/22105/959

Sunny Kumar CSE/22104/958

Sourav Roy CSE/22099/XXX

Mentor - Dr. Soumen Pandit

RSA(Rivest-Shamir-Adleman) Algorithm

1 I will take two large prime number p=3 and q=11.
2. find n=p*q
n=3*11=33 where n is the modules of both public key and private key.
3 $\phi(n)=(p-1)\times(q-1)$ where $\phi(n)$ is the number of coprime it is used for finding the value of e.
$\phi(n)=2*10=20$
4 1< e < 20
finding the value of form {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19} of coprime of 20 and 33.
and e is the value of coprime of 20 and 33 form this set {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19}
so the value of e = { 7, 13, 17, 19}.
5 I will take e=7
public key = (e, n) {formula of public key}
so, public key= (7, 33)
6 e*d mod n = 1 {formula of find d}
7*d mod n = 1
If i will take d=3 then e*d mod n is 1 so R.H.S=L.H.S
7 private key = (d, n) {formula of private key}
then find private key = (3, 33)

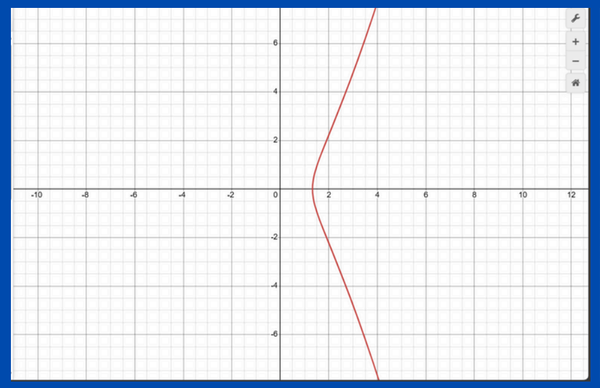
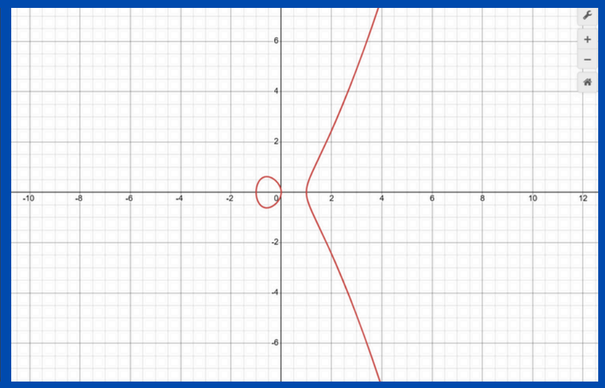
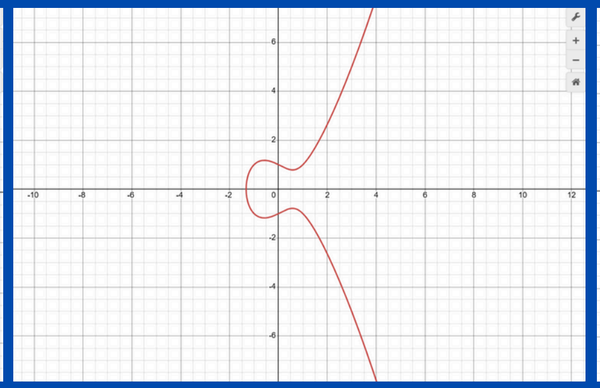
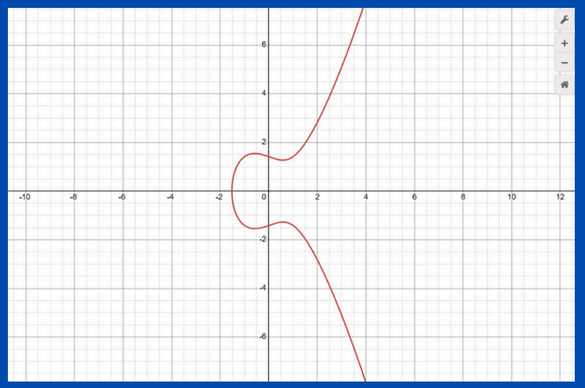
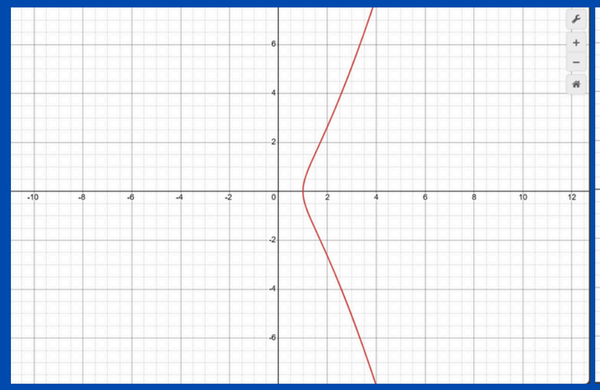
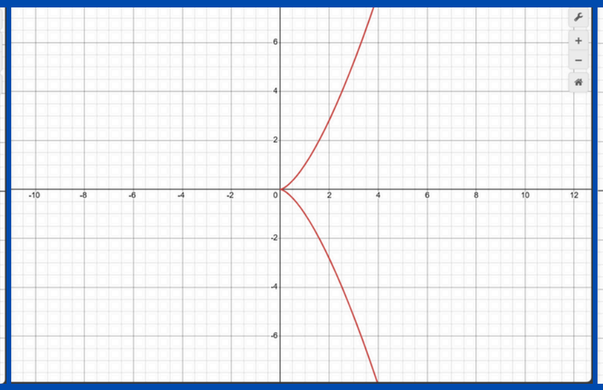
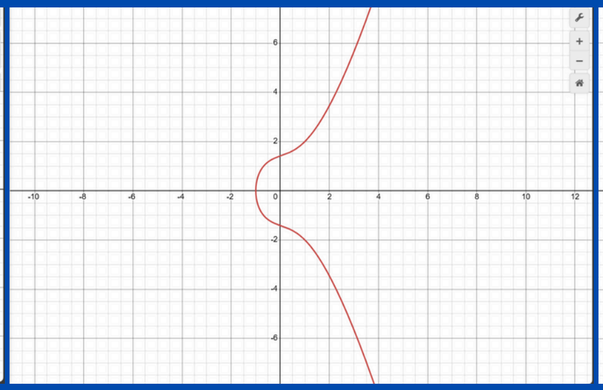
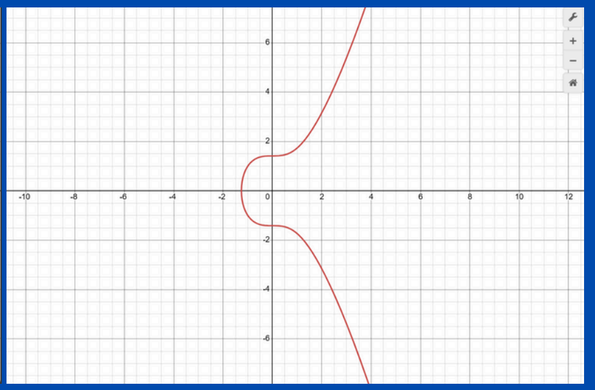
→ example
encrypted value of d is 5
from above public key = (7, 33)
and private key = (3, 33)
c=m^e mod n ciphertext formula
c=5^7 mod 33
c= 78125 mod 33
c=14
m=c^d mod n Plaintext formula
m=14^3 mod 33
m=5

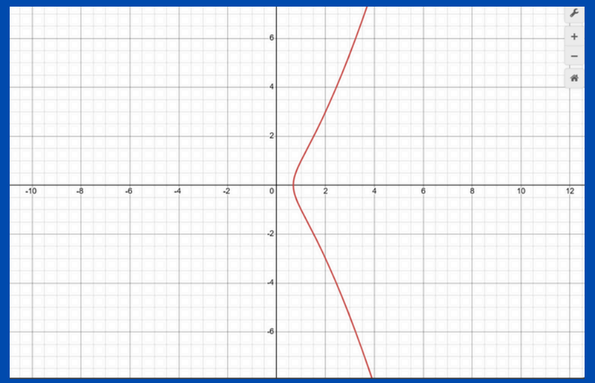
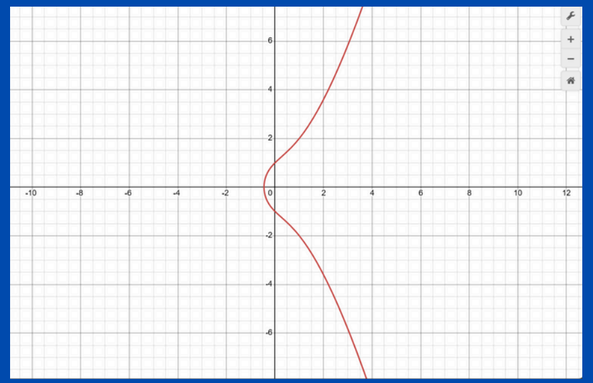
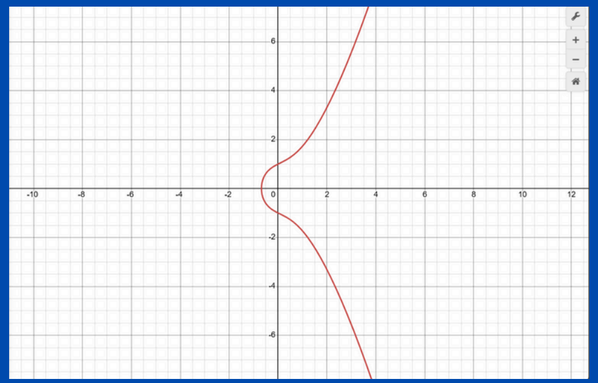
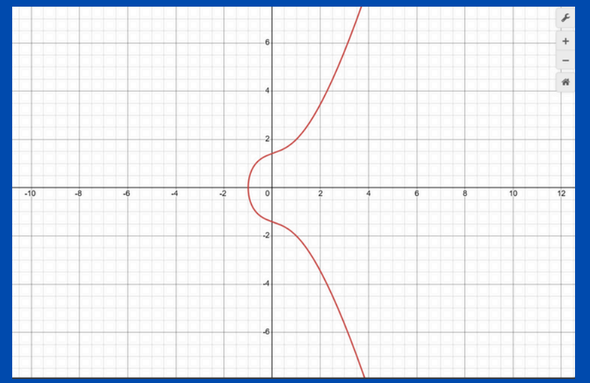
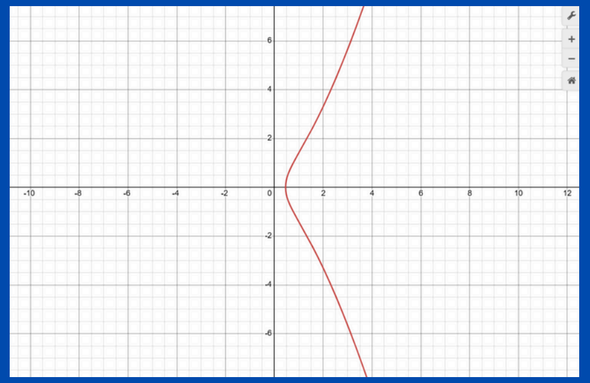
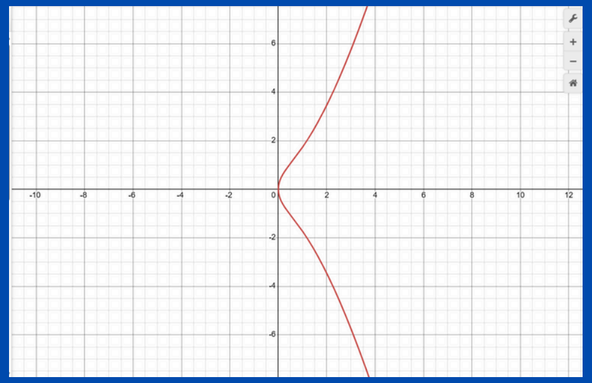
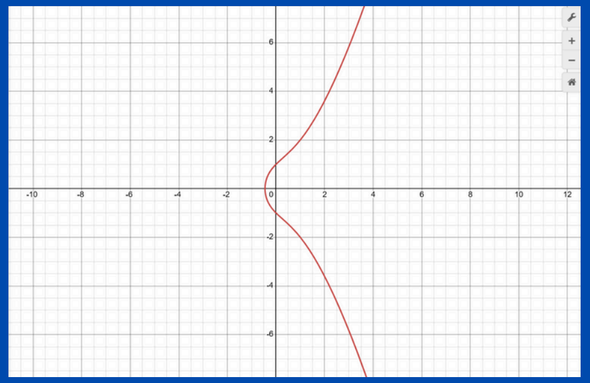
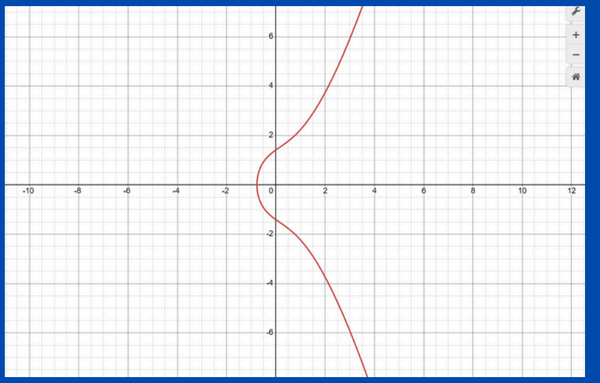
Advantages and Disadvantages of RSA

Advantages	Disadvantages
Strong Security (for large key sizes): RSA is a well-established cryptographic algorithm that provides strong security when using sufficiently large key sizes.	**High Computational Cost**: RSA requires large key sizes (e.g., 2048-bit or 3072-bit) for strong security, making encryption and decryption slower compared to ECC.
Widespread Adoption and Compatibility: RSA is widely supported across many applications, protocols (e.g., TLS, SSL), and legacy systems, ensuring interoperability.	**Large Key Size Requirement**: To maintain security against modern attacks, RSA requires significantly larger key sizes compared to ECC, leading to increased storage and processing overhead.
Simple and Well-Understood Algorithm: RSA is easier to implement and analyze compared to more mathematically complex cryptographic methods like ECC.	**Vulnerability to Quantum Computing**: Future quantum computers could break RSA encryption using Shor's algorithm, making it less future-proof than post-quantum cryptographic alternatives.

Advantages and Disadvantages of Elliptic Curve Cryptography

Advantages	Disadvantages
Higher Security with Smaller Key Sizes: ECC provides the same security level as RSA but with much smaller key sizes (e.g., a 256-bit ECC key is equivalent to a 3072-bit RSA key).	**Complex Implementation**: ECC is more mathematically complex than RSA, making implementation more challenging and prone to errors if not done correctly.
Lower Computational Overhead: Due to smaller key sizes, ECC requires less computational power, making it faster and more efficient, especially for low-power devices like IoT and mobile devices.	**Patent and Licensing Issues**: Some ECC algorithms were historically covered by patents, creating legal concerns for implementations. However, most patents have now expired.
Better Performance in Resource-Constrained Environments: ECC is well-suited for devices with limited processing power, memory, and battery life, such as embedded systems and smart cards.	**Compatibility Issues**: ECC is not as widely supported as RSA in some legacy systems, leading to interoperability challenges.

a \ b	-1	0	1	2
-1				
0				

a \ b	-1	0	1	2
1				
2				

Brief Explanation of Elliptic Curves

The set of points on an elliptic curve form a **group** under elliptic curve point addition.

What is a group ?

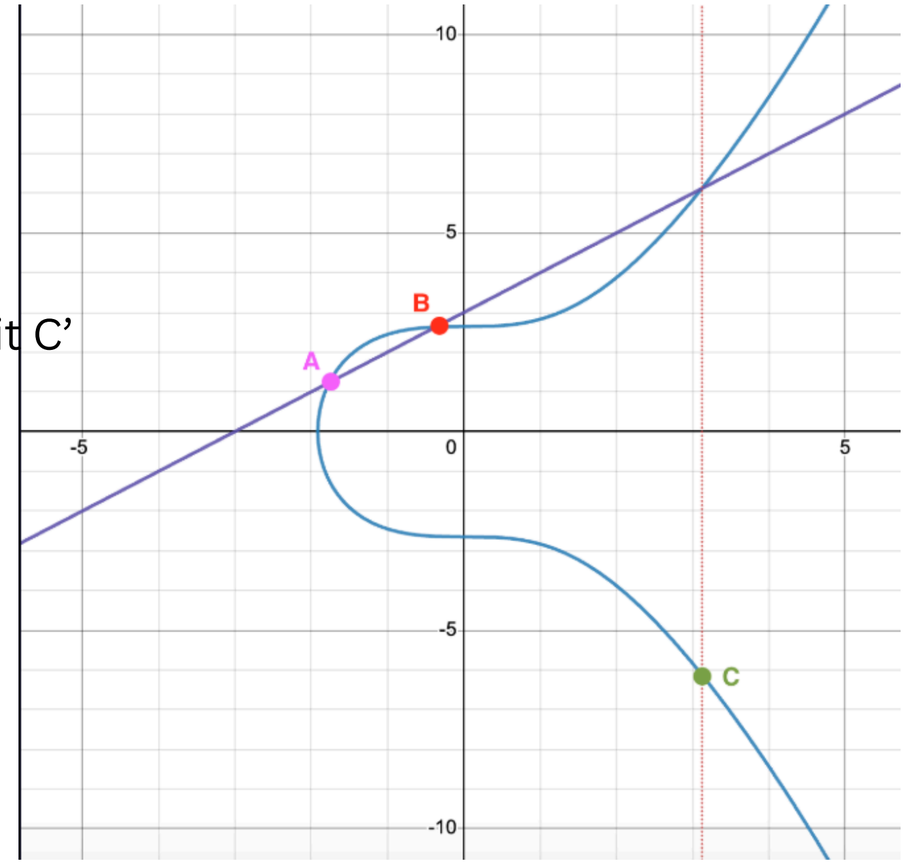
Specifically, to be a group, the set of points needs to have:

- a binary operator that is closed and associative, i.e. it produces another point in the set
- the set must have an identity element I
- every point in the set must have an inverse such that when the two are combined with the binary operator, the result is I

The Binary Operator of Elliptic Curve (Known as Addition)

The Addition here is not the regular addition operation that we do with real numbers . We can define this operator as we want to satisfy the constraints on a group.

- Suppose we take two points on the curve, A and B
- Draw a line passing through the points A and B
- The line will intersect the curve at a third point on the curve, lets say it C’
- Now take the reflection of C’ and lets say it C
- Finally the result of adding the points A and B will be C



Note : In case A=B, the line will be a tangent and it will intersect the curve at a point and rest of the rules for addition is same

Formula for point addition

Using some algebra, and given two points

$$P_1 = (x_1, y_1)$$

$$P_2 = (x_2, y_2)$$

One can derive how to compute $P_3 = (x_3, y_3)$ where $P_3 = P_1 \oplus P_2$ using the following formula.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_3 - x_1) - y_1$$

Why taking the reflex of the point ?

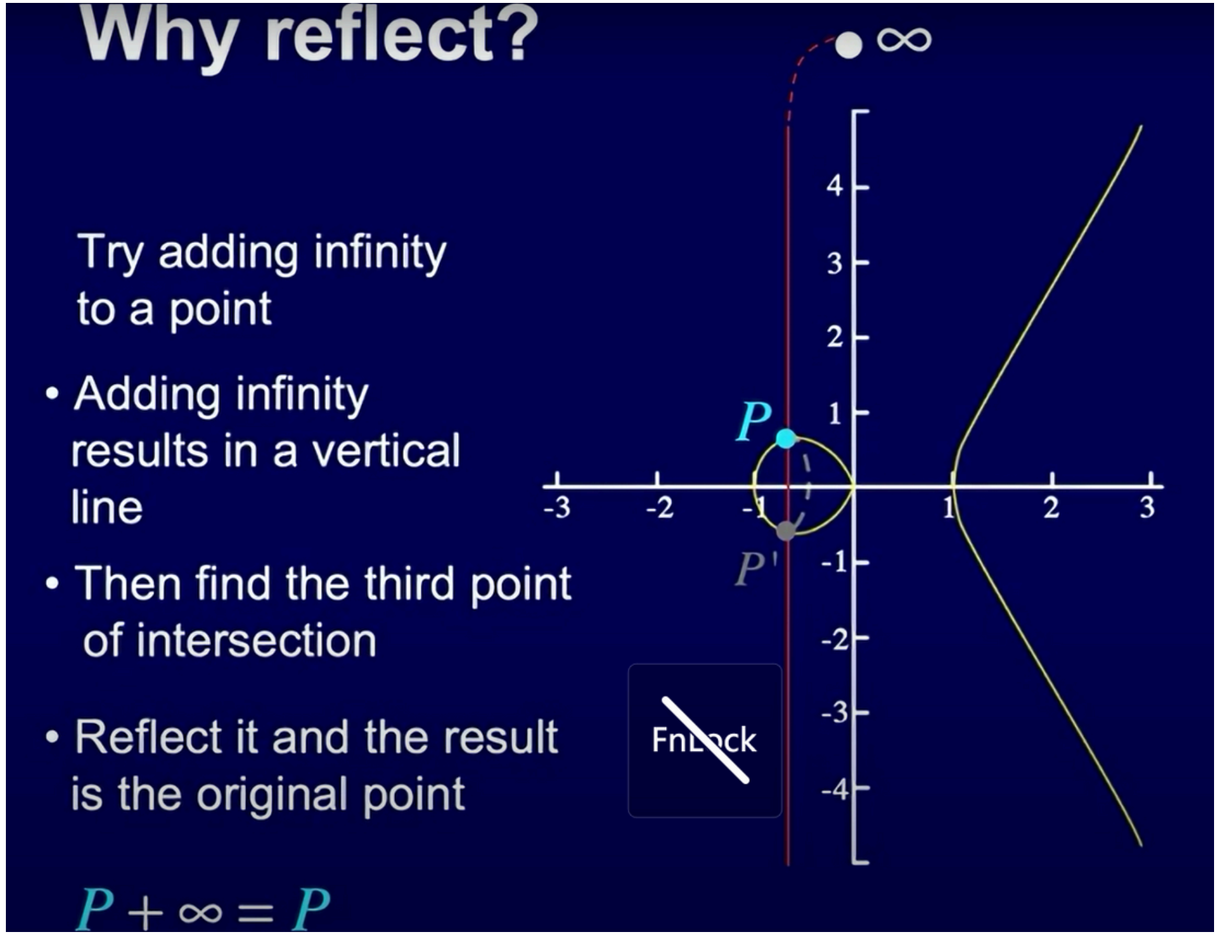
Using our definitions above, the following must be true

$$A \oplus B = C$$
$$A \oplus C = B$$
$$B \oplus C = A$$

With a little algebra, we'll derive a contradiction

$$(B \oplus C) \oplus B = C$$
$$B \oplus C = \text{inv}(B) \oplus C$$
$$B = \text{inv}(B)$$

This says B is equal to it's inverse. But B is not the identity element (which is the only element that can be the inverse of itself), so we have a contradiction.



Note : The inverse of a point on Elilptic curve is the reflection of that point on the curve

Thank You

Sources

https://www.rareskills.io/post/elliptic-curve-addition

https://www.youtube.com/watch?v=XmygBPb7DPM&list=PL8nBmR5eGh37N_BFFj3y35KIBzpSFXmNG