ECC

C R Y P T O G R A P H Y   P R E S E N T A T I O N

Anbuselvan M (22z210)
Vivekanand M U (22z275)
MohamedMuzamil (22z239)
Sridev S (22z262)
Vishnu Barath K (22z274)
Naveen P (23z433)

INTRODUCTION TO ELLIPTIC CURVE CRYPTOGRAPHY

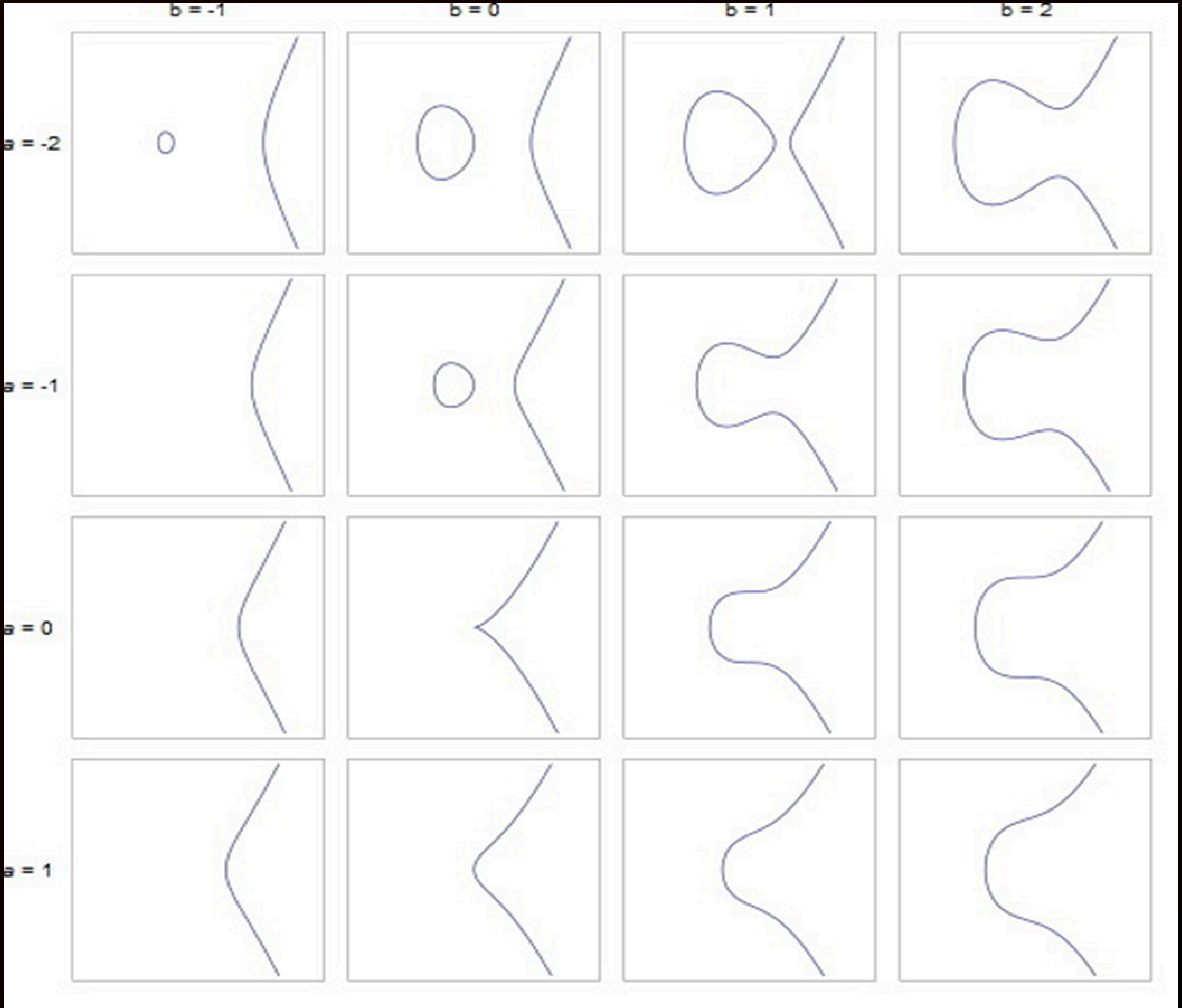
Anbuselvan M - 22Z210

WHAT ARE ELLIPTIC CURVES?

- An elliptic curve over a field K is a non-singular cubic curve in two variables, $f(x,y) = 0$ with a rational point (which may be a point at infinity).

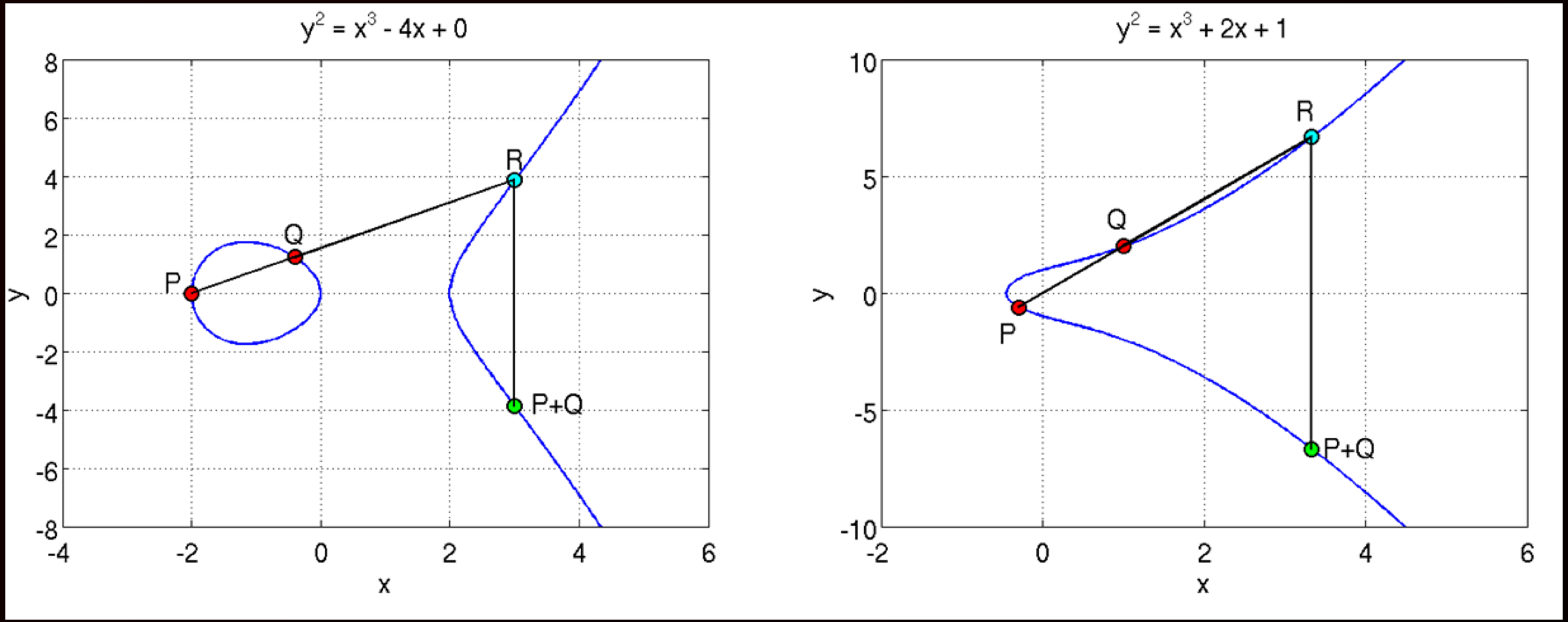
- The field K is usually taken to be the complex numbers, reals, rationals, algebraic extensions of rationals, p-adic numbers, or a finite field.

- Elliptic curves groups for cryptography are examined with the underlying fields of Fp (where $p>3$ is a prime) and F2m (a binary representation with 2m elements).



Examples of Elliptic Curves - $y^2 = x^3 + ax + b$

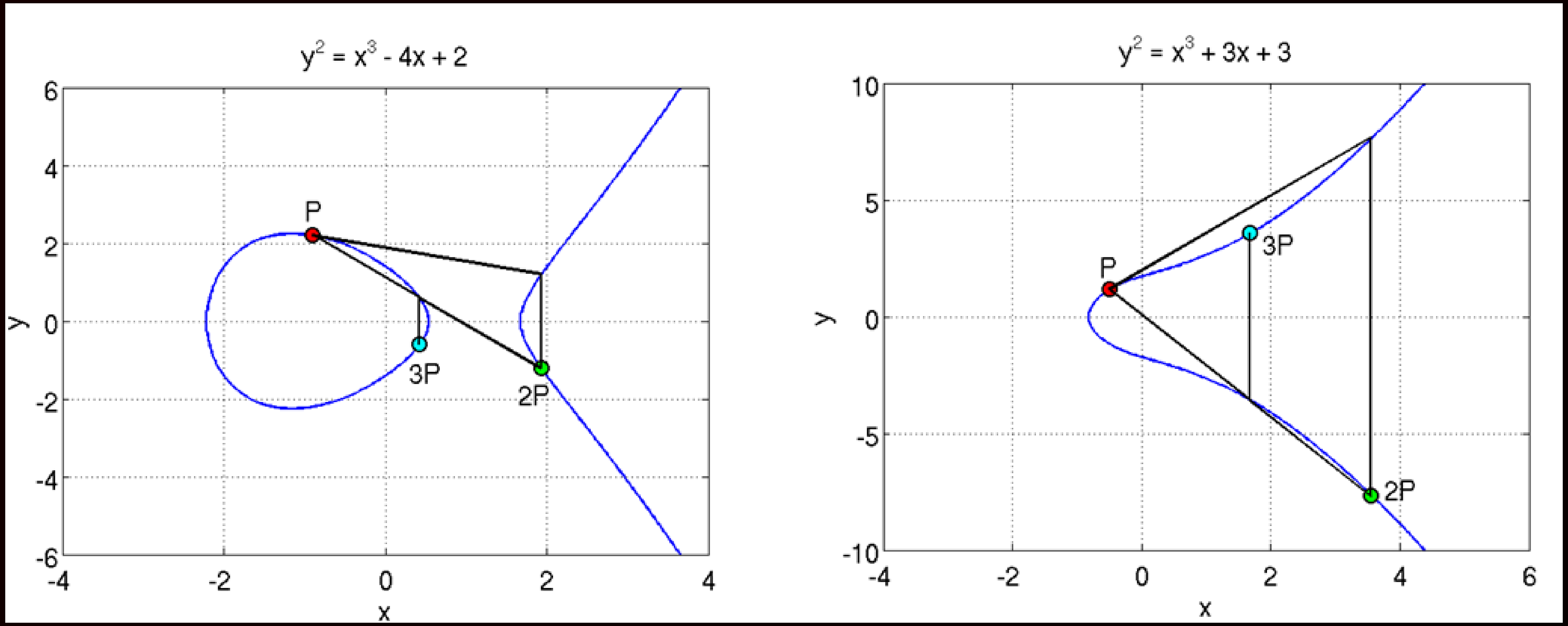
WHAT IS ELLIPTIC CURVE CRYPTOGRAPHY?



Elliptic Curve Point Addition

- Two points P and Q lie on the elliptic curve.
- Draw a line through P and Q, meeting the curve again at R.
- Reflect R across the X-axis to obtain P + Q.
- This defines the elliptic curve addition operation.

WHAT IS ELLIPTIC CURVE CRYPTOGRAPHY?



Point Doubling and Scalar Multiplication

- A tangent at P touches the curve again at a point; its reflection gives 2P.
- Adding P and 2P gives 3P.
- Repeating this gives Q = kP, forming the basis of ECC operations.
- Hard to reverse → ensures cryptographic security.

Point Addition:

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

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1$$

Point Doubling:

$$m = \frac{3x_1^2 + a}{2y_1}$$

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1$$

Formulae

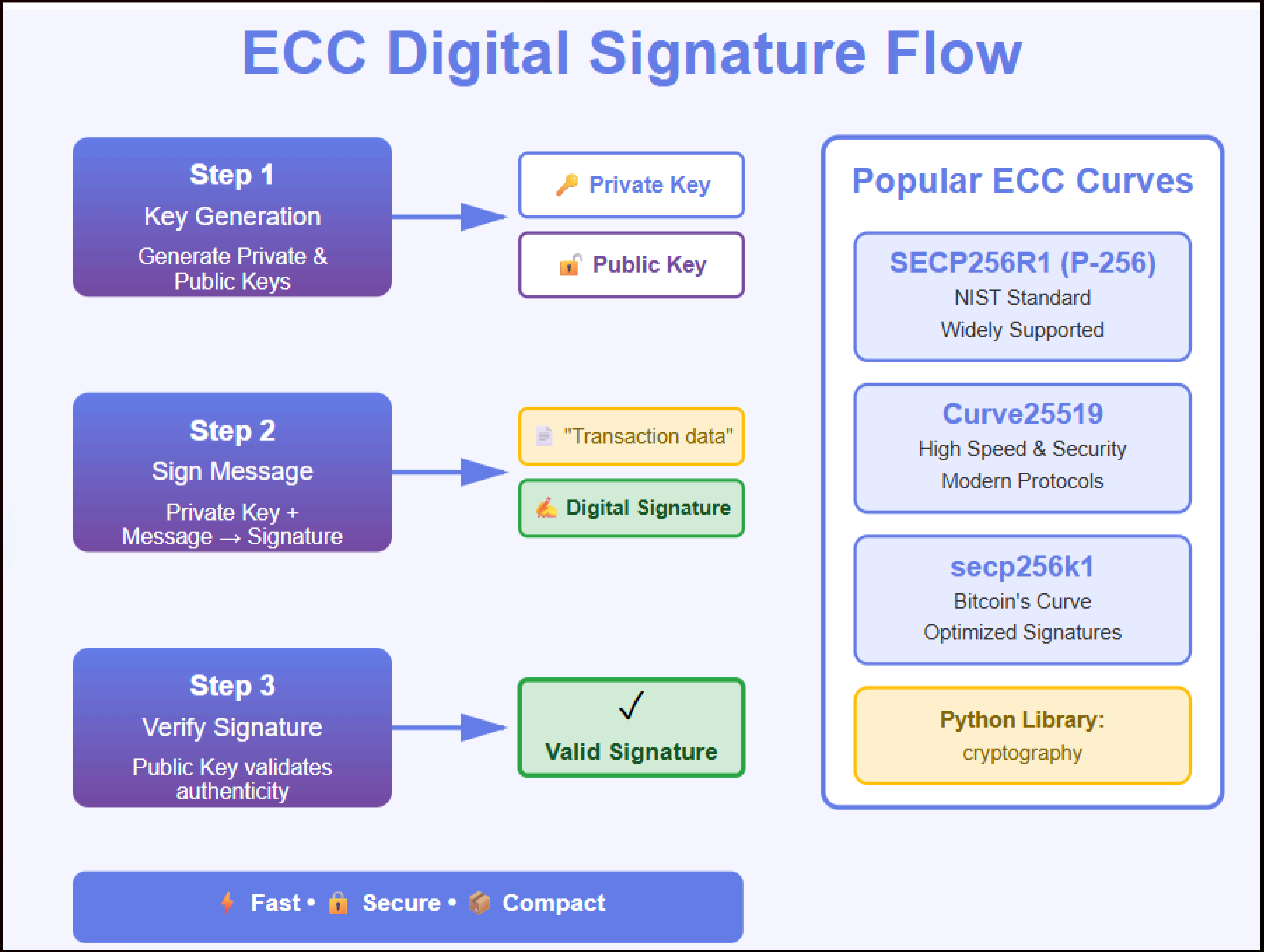
WHAT IS ELLIPTIC CURVE CRYPTOGRAPHY?

<u>Discrete Log Problem</u>

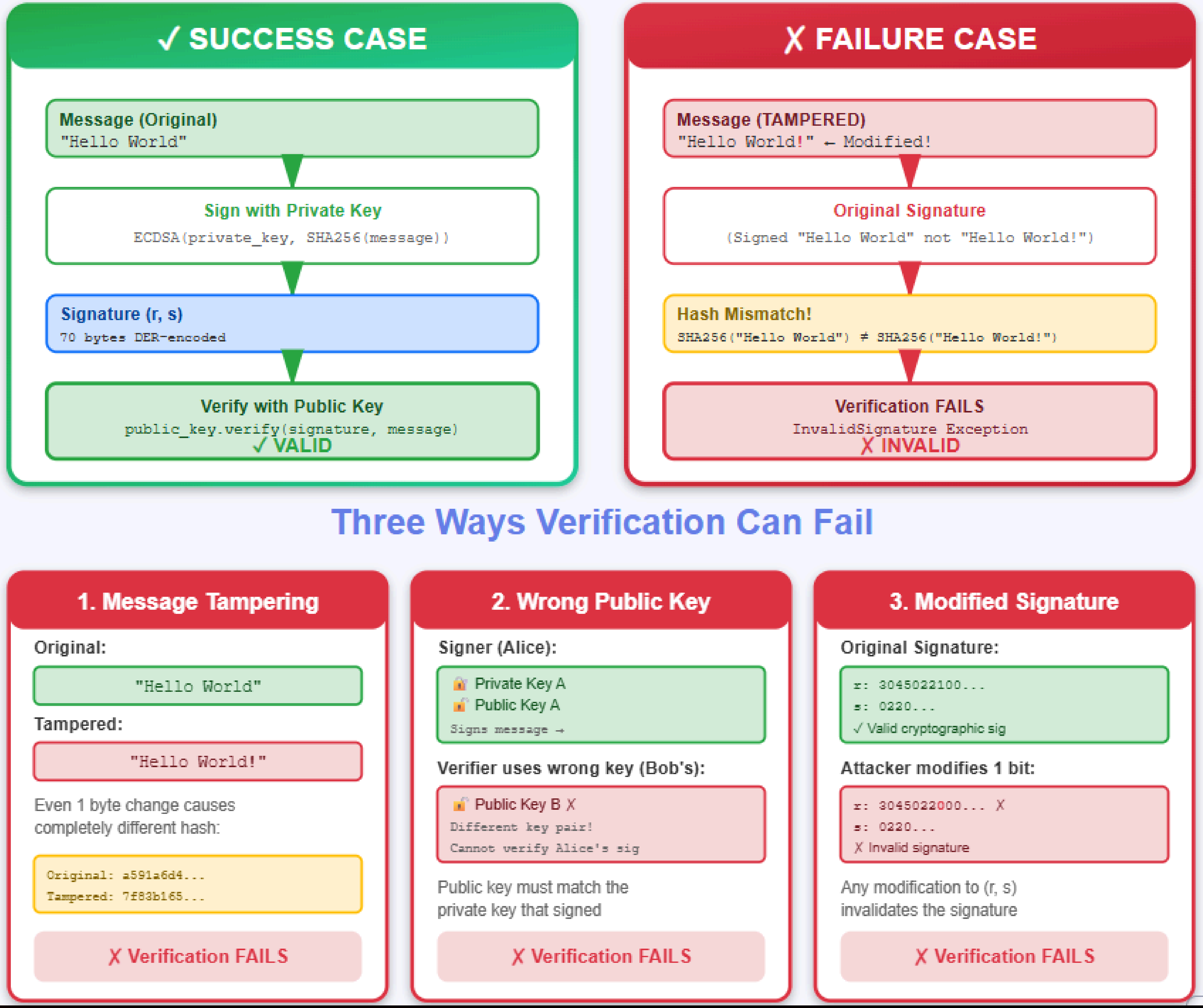
- The security of ECC is due the intractability or difficulty of solving the inverse operation of finding k given Q and P
- This is termed as the discrete log problem
- Methods to solve include brute force and Pollard’s Rho attack both of which are computationally expensive or unfeasible
- The version applicable in ECC is called the Elliptic Curve Discrete Log Problem
- Exponential running time

ECC DIGITAL SIGNATURE & ITS BENEFITS

Vivekanand M U - 22z275


ECC Digital Signature Flow
Step 1
Key Generation
Generate Private & Public Keys
🔑 Private Key
🔓 Public Key
Step 2
Sign Message
Private Key + Message → Signature
"Transaction data"
✍ Digital Signature
Step 3
Verify Signature
Public Key validates authenticity
✓
Valid Signature
Popular ECC Curves
SECP256R1 (P-256)
NIST Standard
Widely Supported
Curve25519
High Speed & Security
Modern Protocols
secp256k1
Bitcoin's Curve
Optimized Signatures
Python Library:
cryptography
⚡ Fast • 🔒 Secure • 📦 Compact

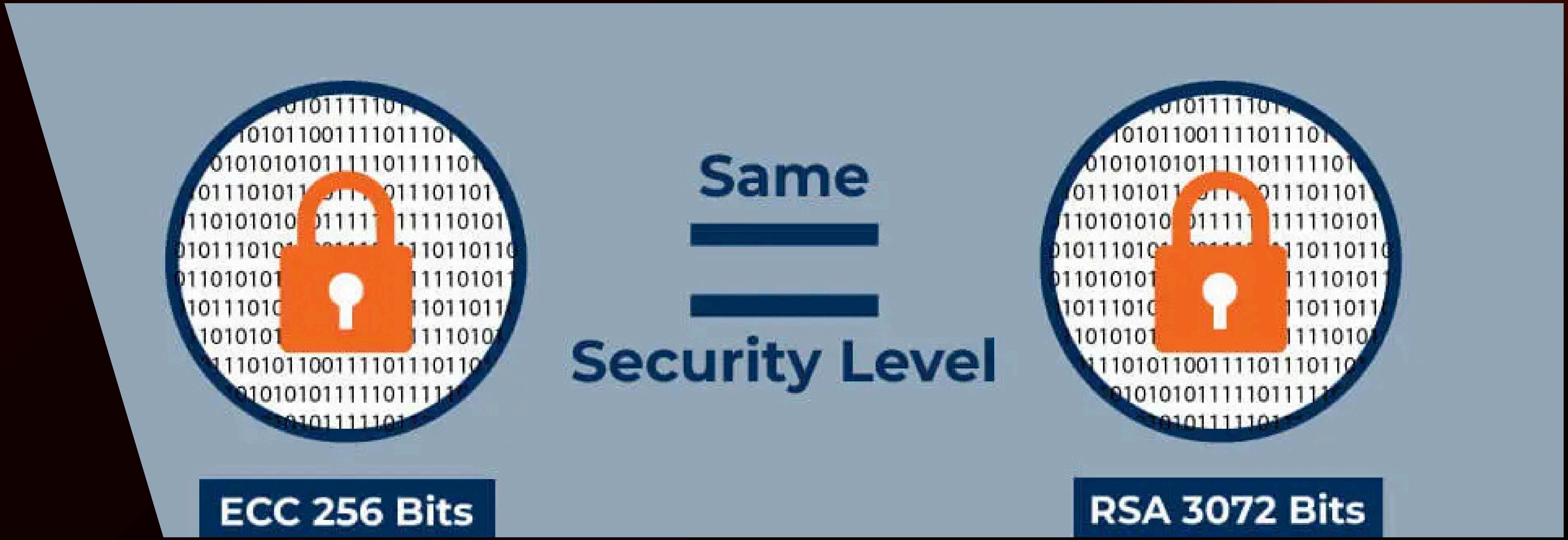
Signature Verification: Success vs Failure Scenarios



```python
# Message
message = b"Hello World"

# Generate ECC Key Pair (SECP256R1)
private_key = ec.generate_private_key(ec.SECP256R1(), default_backend())
public_key = private_key.public_key()

# Export keys (PEM format)
private_pem = private_key.private_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PrivateFormat.PKCS8,
    encryption_algorithm=serialization.NoEncryption()
)
public_pem = public_key.public_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PublicFormat.SubjectPublicKeyInfo
)

# Sign the message
signature = private_key.sign(message, ec.ECDSA(hashes.SHA256()))

# Verify the signature
public_key.verify(signature, b"Hello World", ec.ECDSA(hashes.SHA256()))
```

- Private_key is a random integer d (256-bit for SECP256R1). Public key Q = dG (G = curve generator).
- Keys are serialized in PEM (textual base64) for storage/transmission.
- signature = sign(message, ECDSA(SHA256)) computes (r, s) from hashed message using curve arithmetic.
- verify() checks (r, s) against message hash and public key.

BENEFITS OF ECC



01 Smaller Key Sizes

- 256-bit ECC = 3072-bit RSA in security.
- Reduces storage requirements dramatically.

02 Faster Performance

- Faster encryption/decryption.
- Rapid digital signatures.

03 Lower Bandwidth

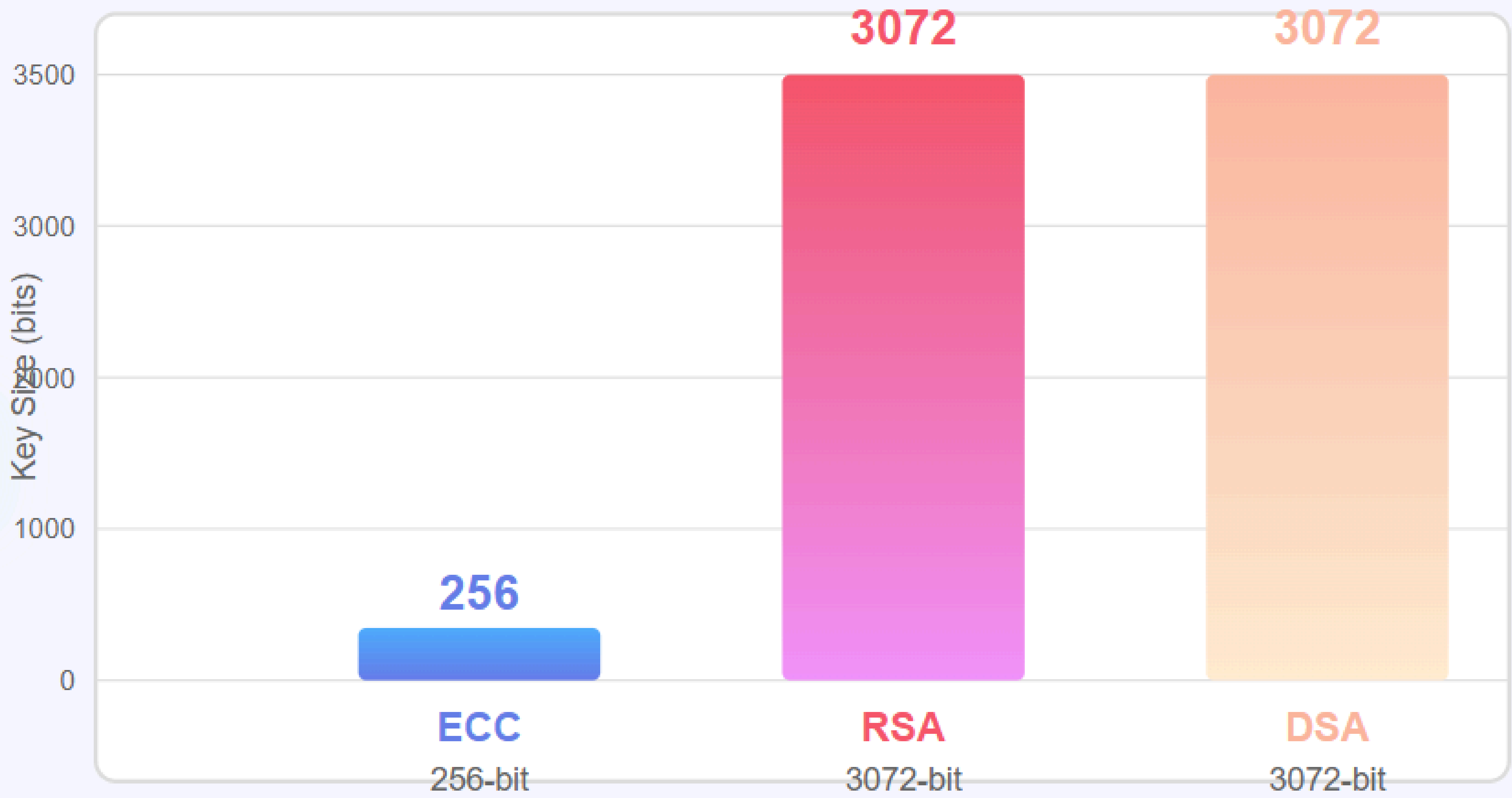
- Reduced network overhead.
- Perfect for mobile networks.

04 Scalable Security

- Easy to increase key size if needed.
- Better future-proofing than RSA

Key Size Comparison

For Equivalent Security Level



ECC is 12x smaller with same security!

ECC in Real-World Applications

PROBLEM 1

Mohamed Muzammil J - 22Z239

PROBLEM

In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is 2P if P = (4, 3.464)?

FROM THE DOUBLING FORMULAE:

$P + P = 2P$

$P = (4, 3.464) = (X_P, Y_P)$

$Y^2 = X^3 + AX + B \implies Y^2 = X^3 - 17X + 16$

$A = -17$

$$S = (3X_P^2 + A) / (2Y_P)$$

$S = (3*(4)^2 + (-17)) / 2*(3.464)$

$= 31 / 6.928 = 4.475$

$X_R = S^2 - 2X_P$

$= (4.475)^2 - 2(4)$

$= 20.022 - 8 = 12.022$

$Y_R = -Y_P + S(X_P - X_R)$

$= -3.464 + 4.475(4 - 12.022)$

$= -3.464 - 35.898 = -39.362$

THUS 2P = (12.022, -39.362)

PROBLEM 2

Sri Dev S - 22z262
Vishnu Barath - 22z274

PROBLEM :

What is the Discrete Logarithm problem for elliptic curves?

The cryptosystem parameters are

E67(2,3), a=2, b=3 and G=(2,22). B's secret key nB=4.

a. Find B's public key PB.

b. A wishes to encrypt the message Pm=(24,26) and chooses the random value k=3.Determine the cipher text C_m.

a. Find B's public key P_B.

Compute B's public key PB = nBG = 4G

Step 1 — compute 2G=G+G(doubling G=(2,22))

$$s = (3x_P^2 + a) / (2y_P)$$

$$3x1^2+a = 3 \cdot (2)^2+2 = 3 \cdot 4+2 = 14.$$

$$2y1=2 \cdot 22=44.$$

$$44^{-1}(\mathrm{mod}67)=32.$$

$$\lambda=14 \cdot 32(\mathrm{mod}67) = 448(\mathrm{mod}67) = 46.$$

$$
\begin{aligned}
x_3 &= \lambda^2 - 2x1 \\
&= 46^2 - 2 \cdot 2 \\
&= 2116 - 4 \\
\mathbf{x_3} &\mathbf{= 2112.}
\end{aligned}
$$

Reduce: $2112 \bmod 67 = 35$.

$$
\begin{aligned}
y_3 &= \lambda(x1 - x3) - y1 \\
&= 46(2 - 35) - 22 \\
&= 46(-33) - 22 \\
&= -1518 - 22 \\
\mathbf{y_3} &\mathbf{= -1540.}
\end{aligned}
$$

Reduce: $-1540 \bmod 67 = 1$.

2G=(35, 1)

Step 3 — compute 4G = 2(2G) (double 2G=(35,1))

$3x_1^2+a = 3 \cdot 35^2+2 = 3 \cdot 1225+2 = 3677.$

$2y1 = 2 \cdot 1 = 2.$

$\lambda = 59.\ 2^{-1}(\mathrm{mod}67) = 34$

$\lambda = 59 \cdot 34(\mathrm{mod}67) = 2006 \ \mathrm{mod}67 = 63.$

$x3 = 63^2-35-35=3969-70 = 3899 \ (\mathrm{mod}\ 67) \equiv 13.$

$y3=63(35-13)-1 = 63 \cdot 22-1 = 1386-1 = 1385 \equiv 45(\mathrm{mod}67).$

4G=(13, 45).

Therefore B’s public key is

PB=4G=(13, 45).

What is the Discrete Logarithm problem for elliptic curves?
The cryptosystem parameters are
$E_{67}(2,3)$, a=2, b=3 and G=(2,22). B's secret key n_B=4.

b. A wishes to encrypt the message Pm=(24,26) and chooses the random value k=3. Determine the cipher text C_m.

ElGamal on EC: ciphertext $C = (C_1, C_2)$ where

$$C_1 = kG, \qquad C_2 = P_m + kP_B.$$

We must compute kG and kP_B.

Compute $kG = 3G$

We already computed $3G = (52, 22)$. So

$$\boxed{C_1 = (52,\ 22).}$$

Compute $kP_B = 3P_B$ where $P_B = (13, 45)$

We'll compute $2P_B$ then $3P_B = 2P_B + P_B$.

Step i — $2P_B = 2(13, 45)$ (doubling)

- Numerator $3x^2 + a = 3 \cdot 13^2 + 2 = 3 \cdot 169 + 2 = 509.$
  - $509 \bmod 67 = 40$ (since $67 \cdot 7 = 469$, remainder 40).
- Denominator $2y = 2 \cdot 45 = 90 \equiv 23 \pmod{67}.$
- Inverse $23^{-1} \pmod{67} = 35$ (because $23 \cdot 35 = 805 \equiv 1$).
- $\lambda = 40 \cdot 35 \pmod{67} = 1400 \bmod 67 = 60.$
- $x_3 = 60^2 - 13 - 13 = 3600 - 26 = 3574 \equiv 23 \pmod{67}.$
- $y_3 = 60(13 - 23) - 45 = 60(-10) - 45 = -600 - 45 = -645 \equiv 25 \pmod{67}.$

So $2P_B = (23,\ 25)$.

Step ii — $3P_B = (23, 25) + (13, 45)$

- Slope numerator = $45 - 25 = 20$.
- Denominator = $13 - 23 = -10 \equiv 57 \pmod{67}$.
- Inverse $57^{-1} \pmod{67} = 20$ (since $57 \cdot 20 = 1140 \equiv 1$).
- $\lambda = 20 \cdot 20 \pmod{67} = 400 \bmod 67 = 65$.
- $x_3 = 65^2 - 23 - 13 = 4225 - 36 = 4189 \equiv 35 \pmod{67}$.
- $y_3 = 65(23 - 35) - 25 = 65(-12) - 25 = -780 - 25 = -805 \equiv 66 \pmod{67}$.

So

$$\boxed{kP_B = 3P_B = (35,\ 66).}$$

Compute $C_2 = P_m + kP_B = (24, 26) + (35, 66)$

- Slope numerator: $66 - 26 = 40.$
- Denominator: $35 - 24 = 11.$
- Inverse: $11^{-1} \pmod{67} = 61$ because $11 \cdot 61 = 671 \equiv 1.$
- $\lambda = 40 \cdot 61 \pmod{67} = 2440 \bmod 67 = 28.$
  (Check: $67 \cdot 36 = 2412$, remainder 28.)
- $x_3 = 28^2 - 24 - 35 = 784 - 59 = 725 \bmod 67 = 55.$
  (Because $67 \cdot 10 = 670$, remainder 55.)
- $y_3 = 28(24 - 55) - 26 = 28(-31) - 26 = -868 - 26 = -894 \bmod 67 = 44.$
  (Because $-894 + 67 \cdot 14 = -894 + 938 = 44$.)

So

$$\boxed{C_2 = (55,\ 44).}$$

Final ciphertext (ElGamal on the curve)

$$\boxed{C = (C_1,\ C_2) = ((52,\ 22),\ (55,\ 44)).}$$

THANK YOU