Digital Signature, Digital Certificates / SSL

&

Elliptic Curve

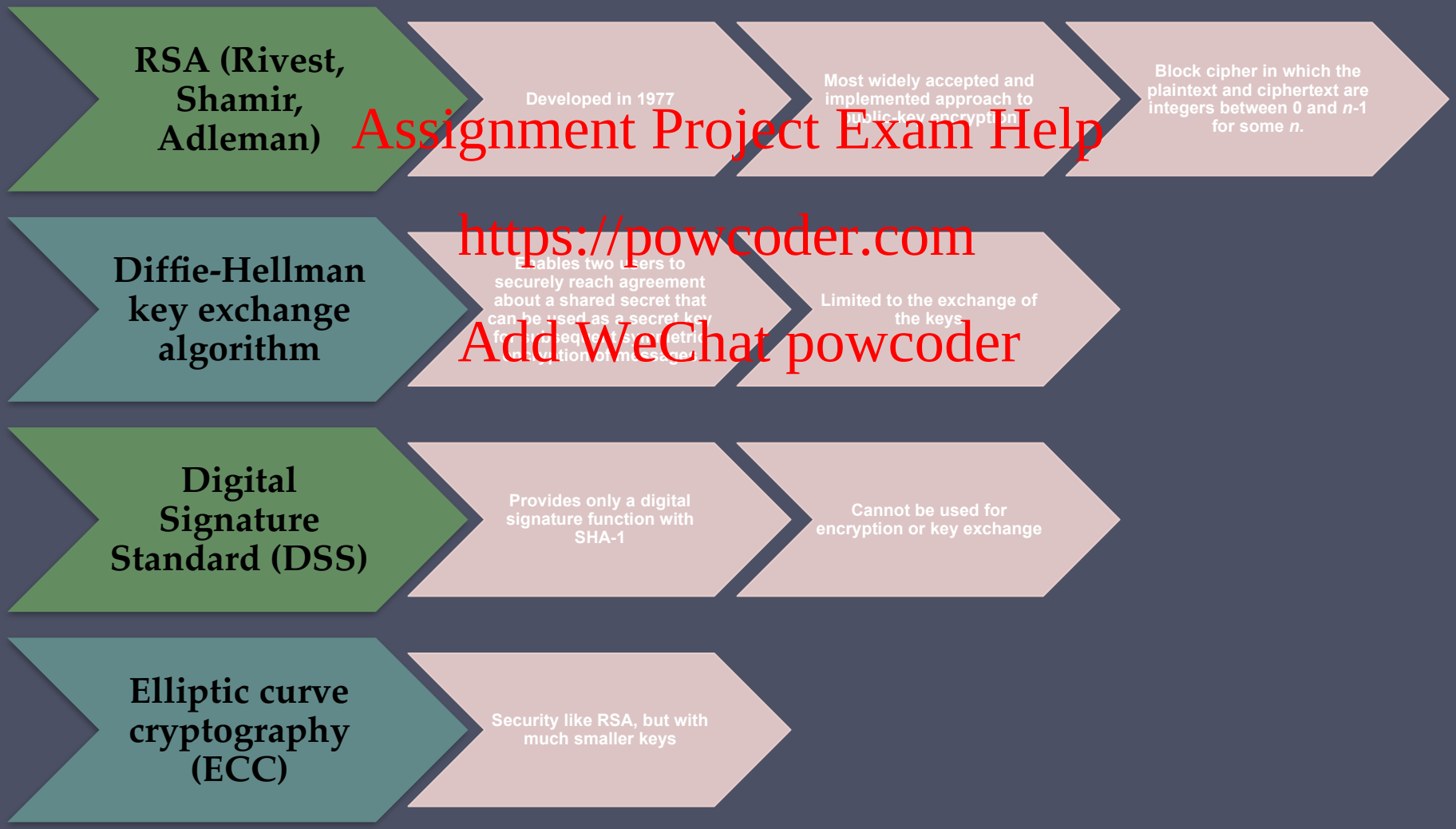
Lecture 5b

Overview

- Asymmetric algorithms
- Digital signatures
- Digital certificate
  - What is a digital certificate?
  - Scenario of digital certificate
  - Types of digital certificates
- PKI – Public Key Infrastructure and digital certificate
- Trust
- Certificate Authority
  - What is CA?
  - Intermediate CAs
  - Browsers and CAs
- SSL/TLS protocol and SSL certificate
- Digital envelope
- Stored Data encryption

- Elliptic curve
  - Fundamentals
  - Bitcoin key generation and ECC
  - Tor network and ECC
  - Applications of ECC

Asymmetric Encryption Algorithms



Digital Signatures

- NIST defines a digital signature as:

> **"The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation."**

- Thus, a digital signature is a data-dependent bit pattern, generated by an agent as a function of a file, message, or other form of data block

- three digital signature algorithms:
  - Digital Signature Algorithm (DSA)
  - RSA Digital Signature Algorithm
  - Elliptic Curve Digital Signature Algorithm (ECDSA)

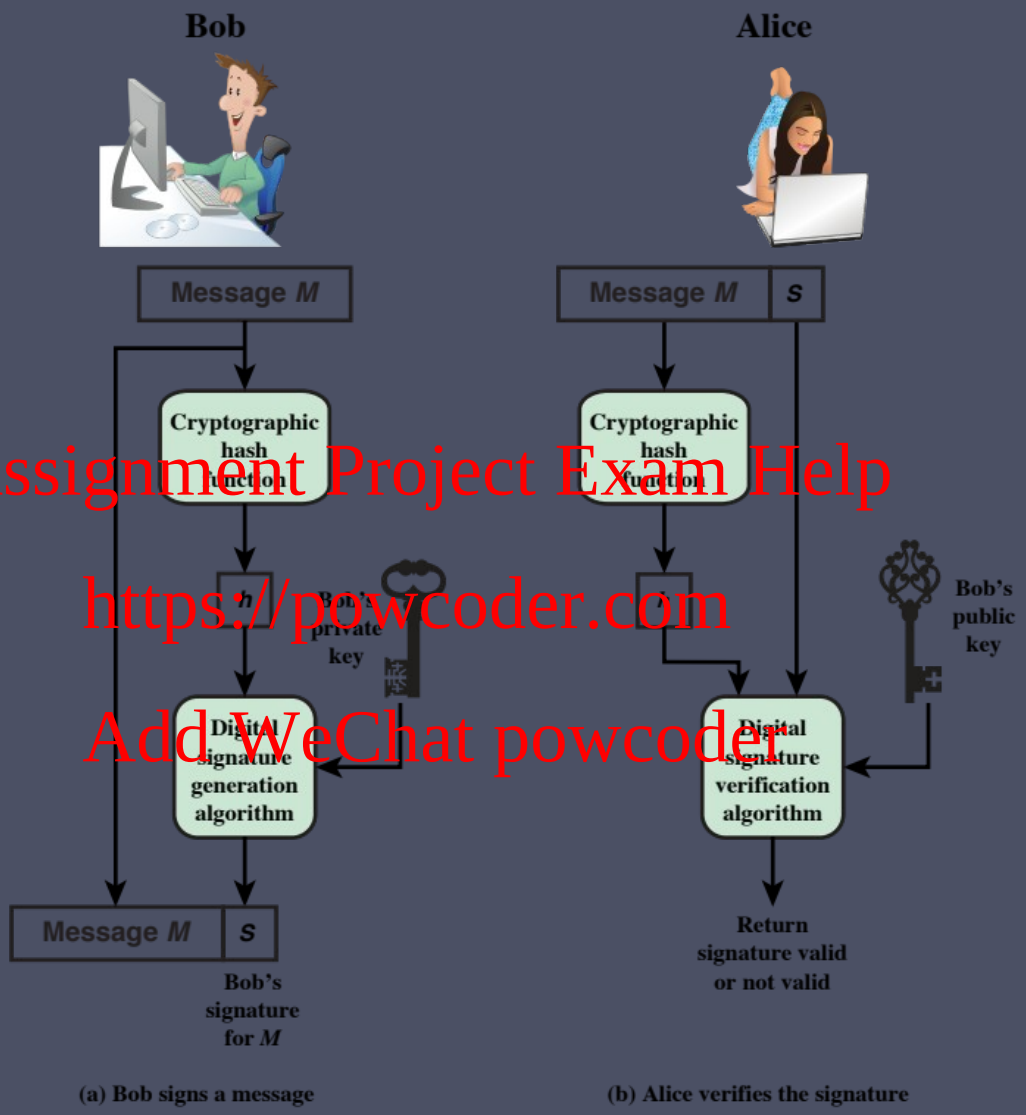


Figure 2.7 Simplified Depiction of Essential Elements of Digital Signature Process

Man-in-the-Middle Attack

- Attack is:
  1. Darth generates private keys X_{D1} and X_{D2}, and their public keys Y_{D1} and Y_{D2}
  2. Alice transmits Y_A to Bob
  3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates K2
  4. Bob receives Y_{D1} and calculates K1
  5. Bob transmits X_A to Alice
  6. Darth intercepts X_A and transmits Y_{D2} to Alice. Darth calculates K1
  7. Alice receives Y_{D2} and calculates K2
- All subsequent communications compromised

Digital Certificate

- A digital certificate is an electronic permit that allows a person, organization or a computer to exchange the information securely over the Internet by using the public key infrastructure (PKI).

- Digital certificates help establish the identity of people or electronic assets.

- They protect online transactions by providing secure, encrypted, online communication.

Digital Certificate

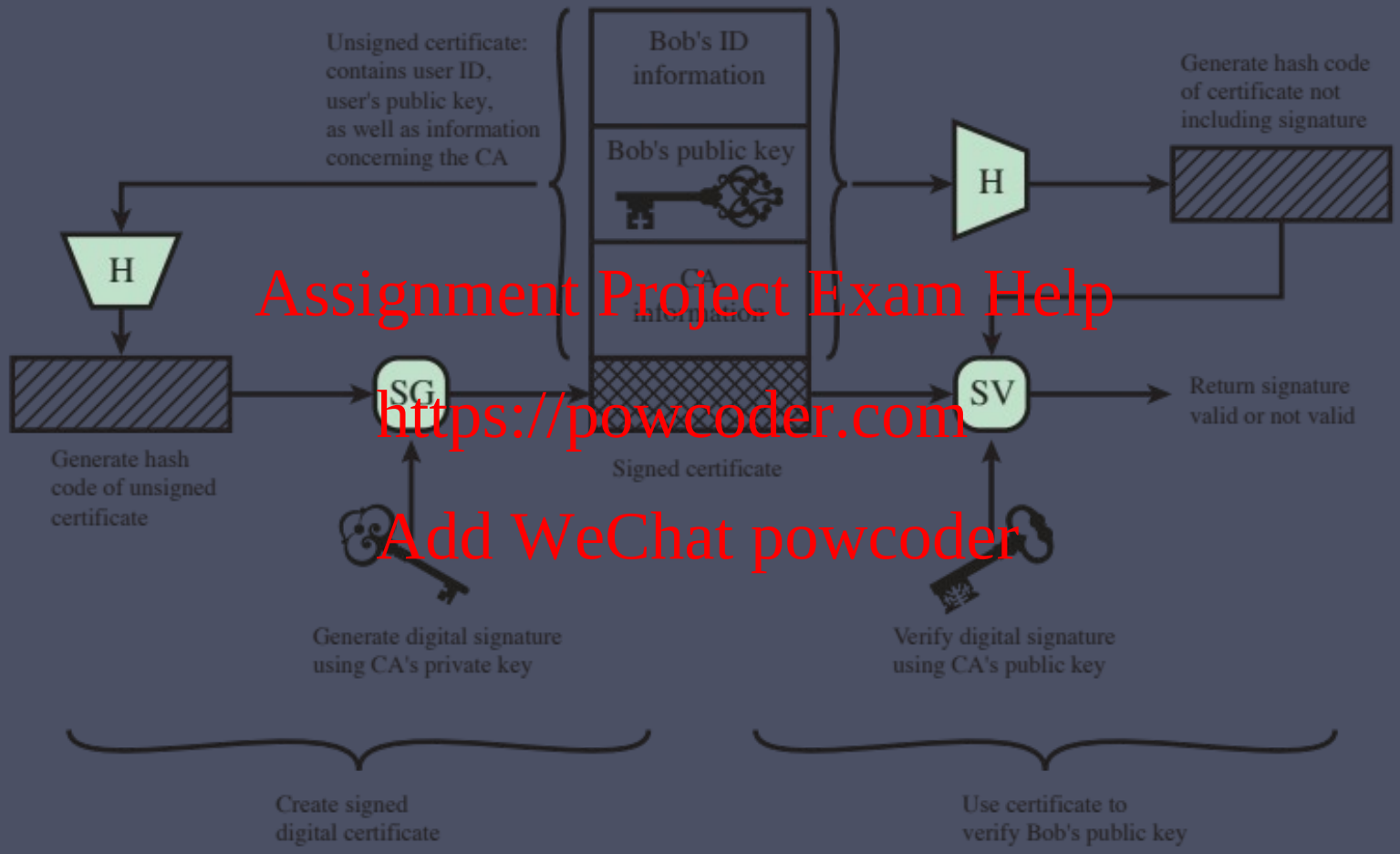


Figure 2.8 Public-Key Certificate Use

Types of digital certificates

SSL certificates

1)Server Certificates : SSL certificate authenticates the server to web browsers

2)Organization Certificates : self-signed certificates

Codesigning certificates

3)Personal Certificates

4)Developer Certificates

- “A Code Signing Certificate authenticates the identity of a software developer or publisher and provides assurance that the signed piece of software has not been altered or tampered with. This is done by applying a digital signature and hashing it along with the software itself.”

- a user attempts to download a piece of unsigned software the browser or antivirus program they’re running will flag it

Public Key Infrastructure - PKI

- Framework for managing digital certificates and public key encryption
- Facility the secure electronic transfer of information over the Internet – transactions, sending/receiving personal details etc
- Consists of policies and standards → Ultimate goal is to build trust

Trust

- Trust: Multi-facet complex concept

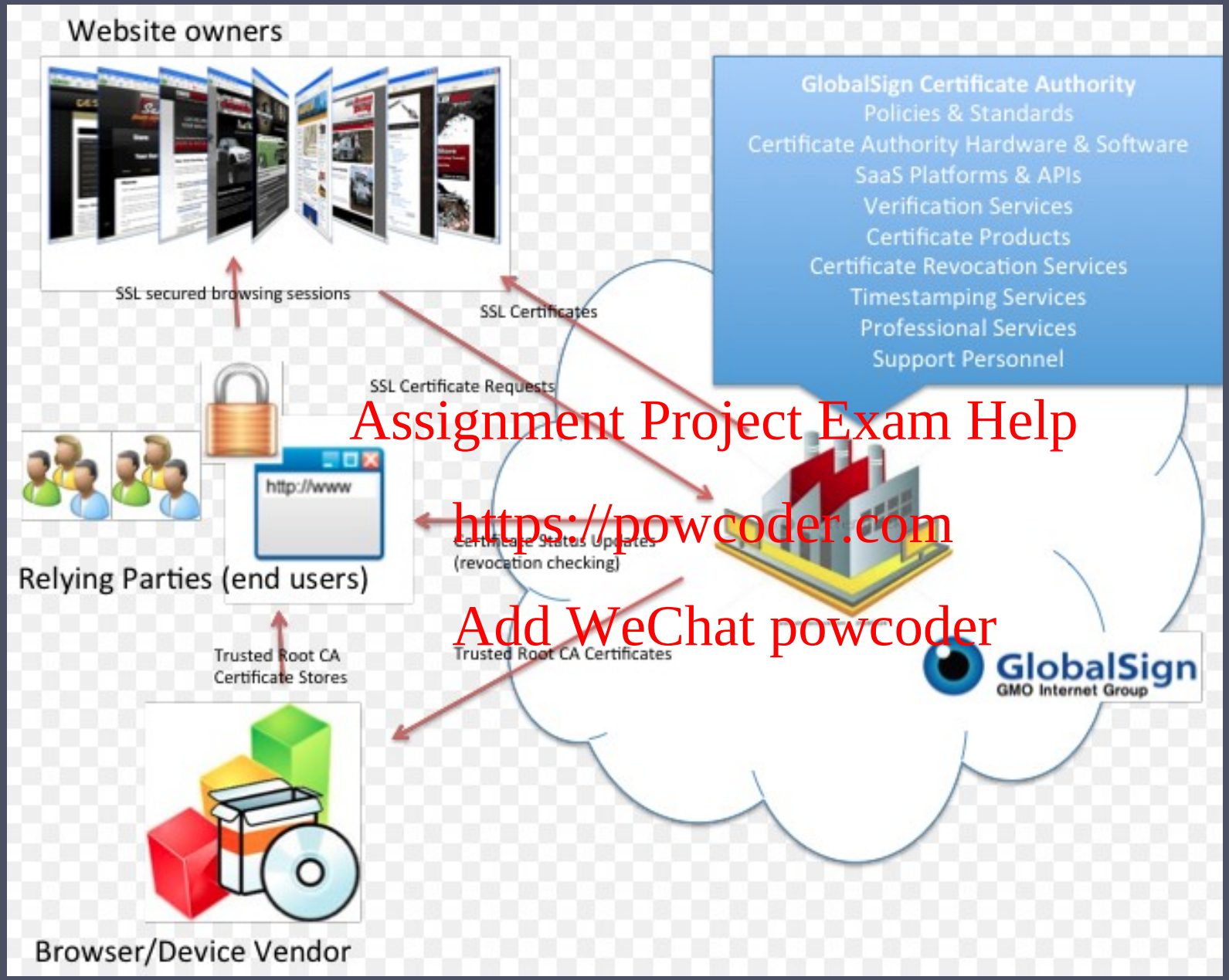
- Trust: Confidence, Benevolence, Reliance
  My research on trust – link
- Frauds in e-commerce: Trust, Identify and Chargeback
  etc

- Interpersonal – direct trust between two

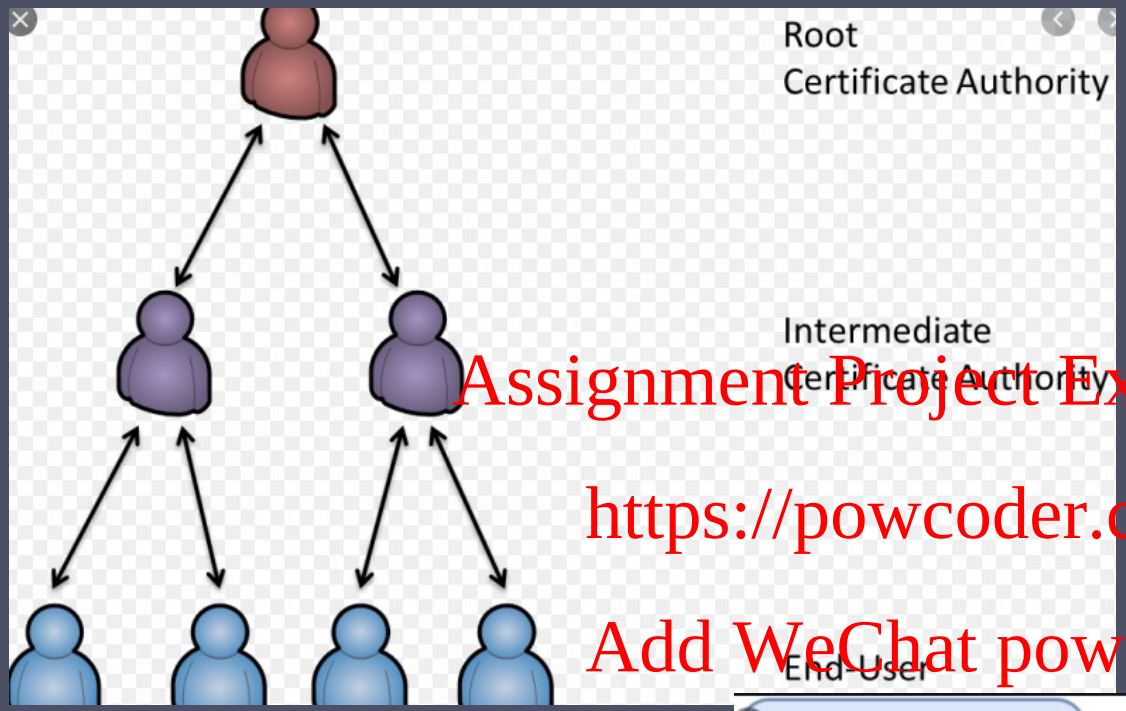
- External – Third party trust
  I trust John, you trust John
  I trust you

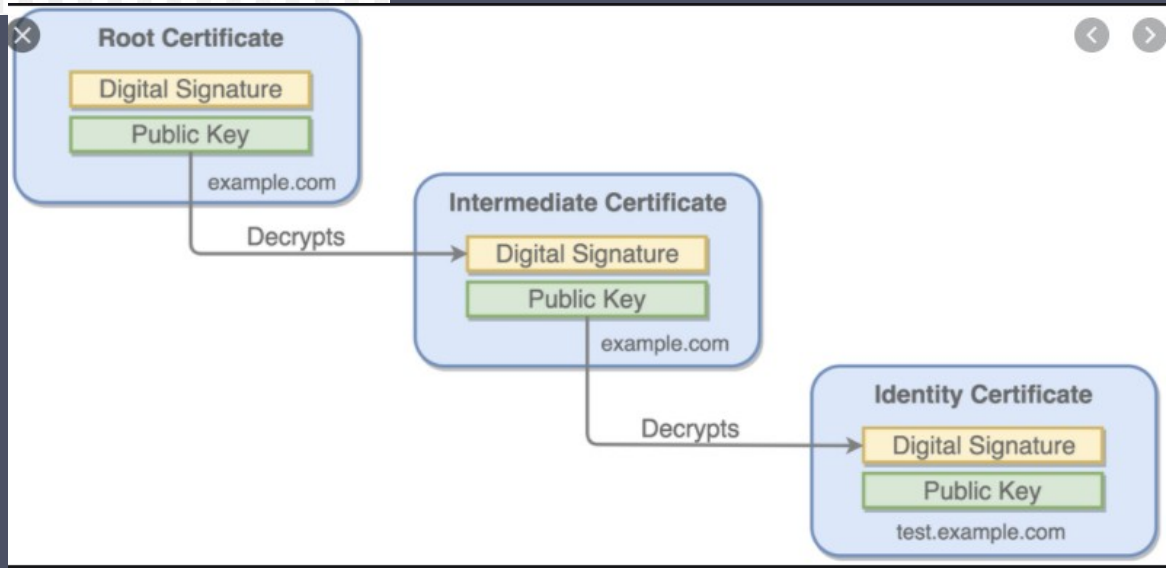
CA

- Certificate Authority
- Certificate Authority or certification authority (CA) is an entity that issues digital certificate. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
- Ensure trust in e-commerce
- Internal to organisation – self signed certificate
- External - Verisgin and GlobalSign are most popular Cas

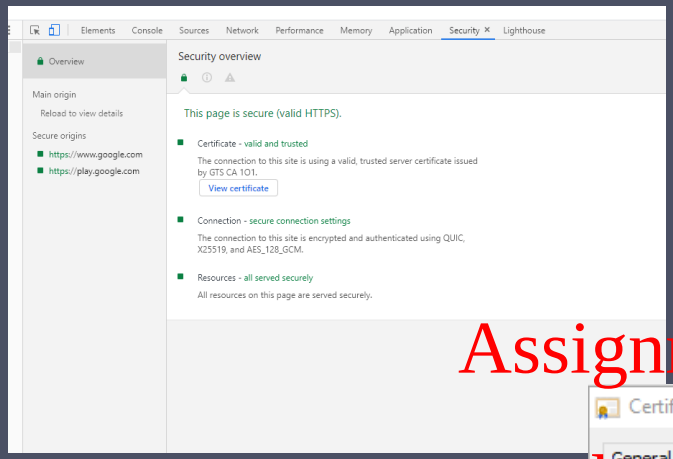


INTERMEDIATE CAs



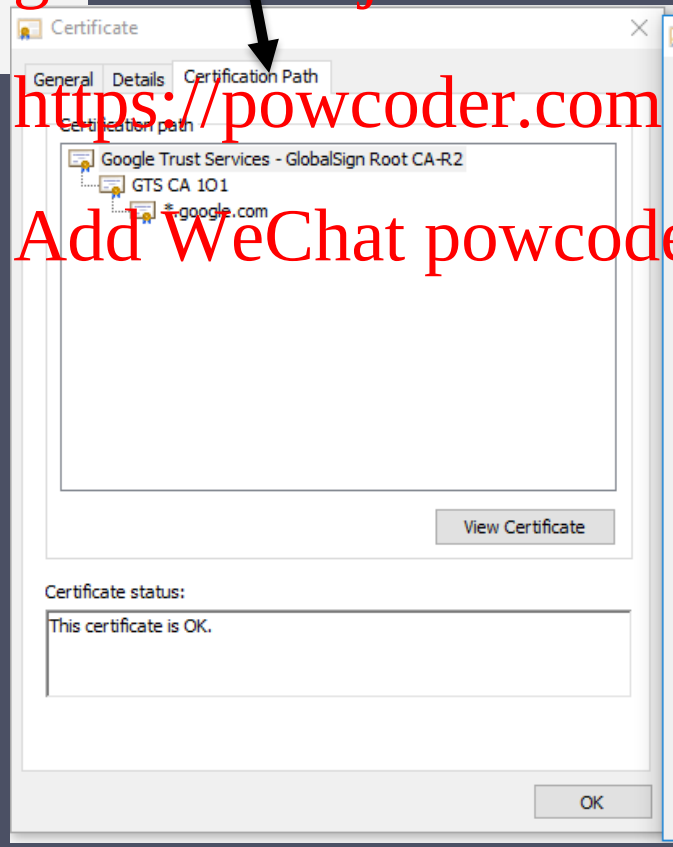


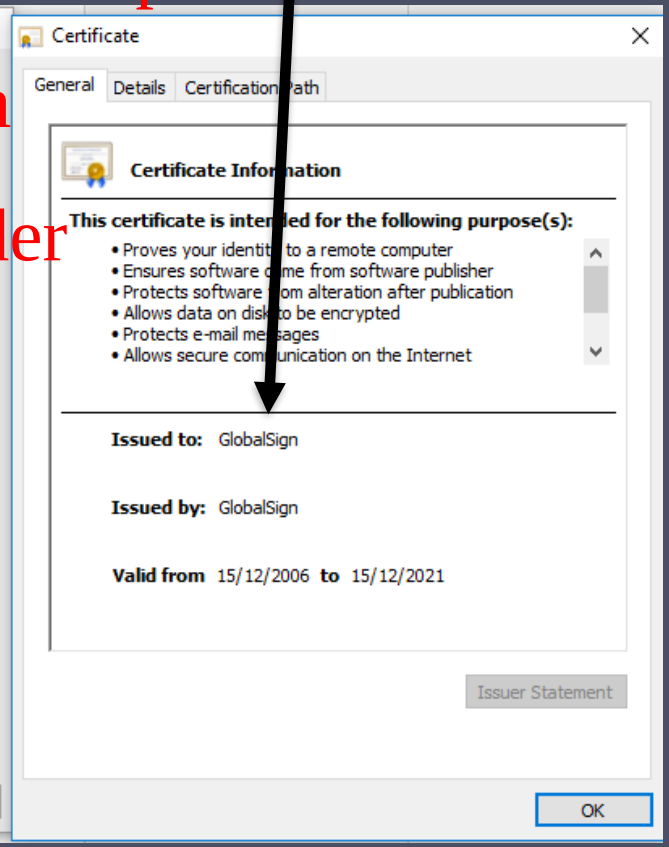
Check certificate with Google connection



Certificate Path, to see root CA

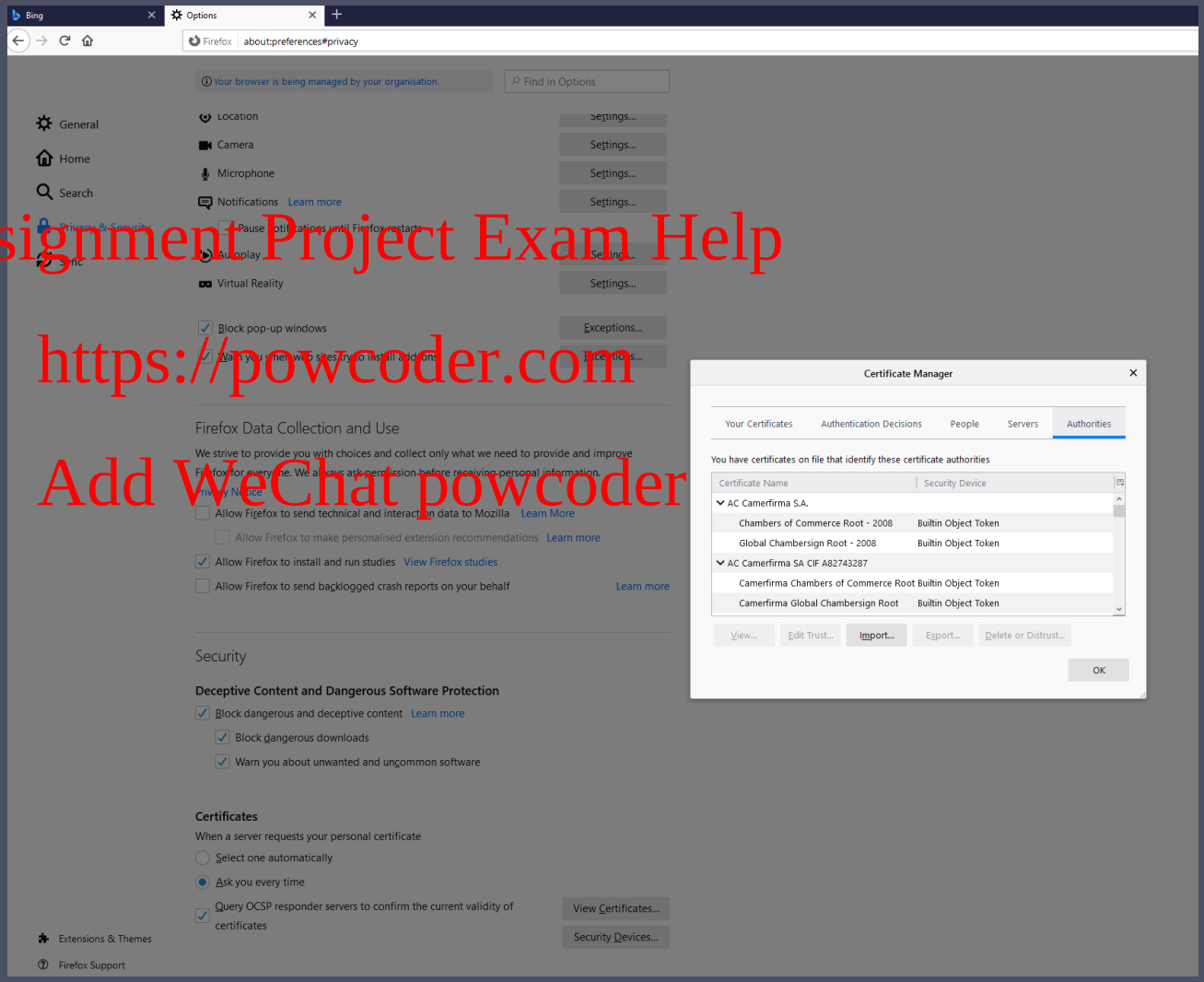
Self-certificate, issue to and issue by same





Browsers - CA

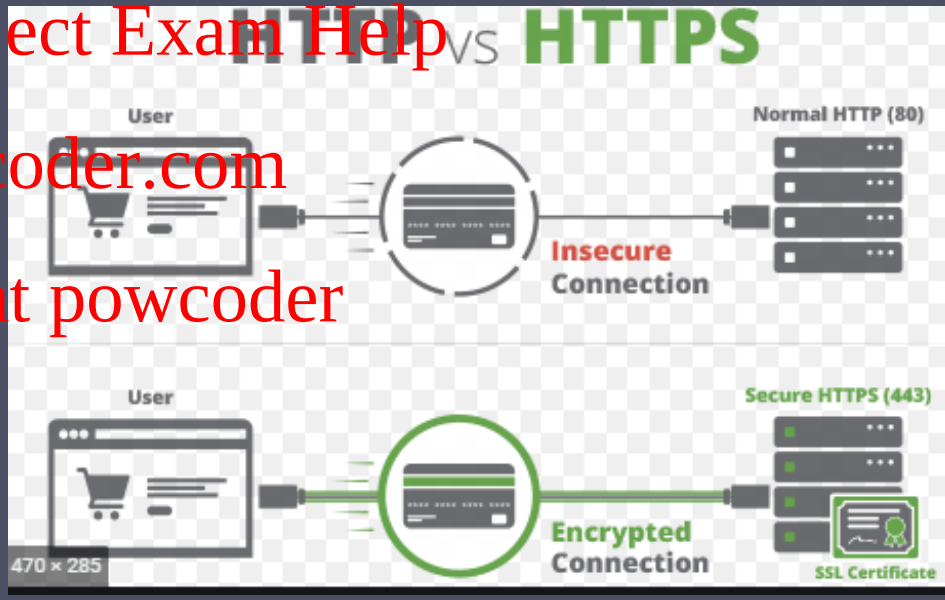
- **Firefox**: Tools > Options > Advanced > Certificates > View Certificates > Authorities.



SSL / TLS

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client

SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely.



More specifically, SSL is a security protocol.

“SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser” GlobalSign

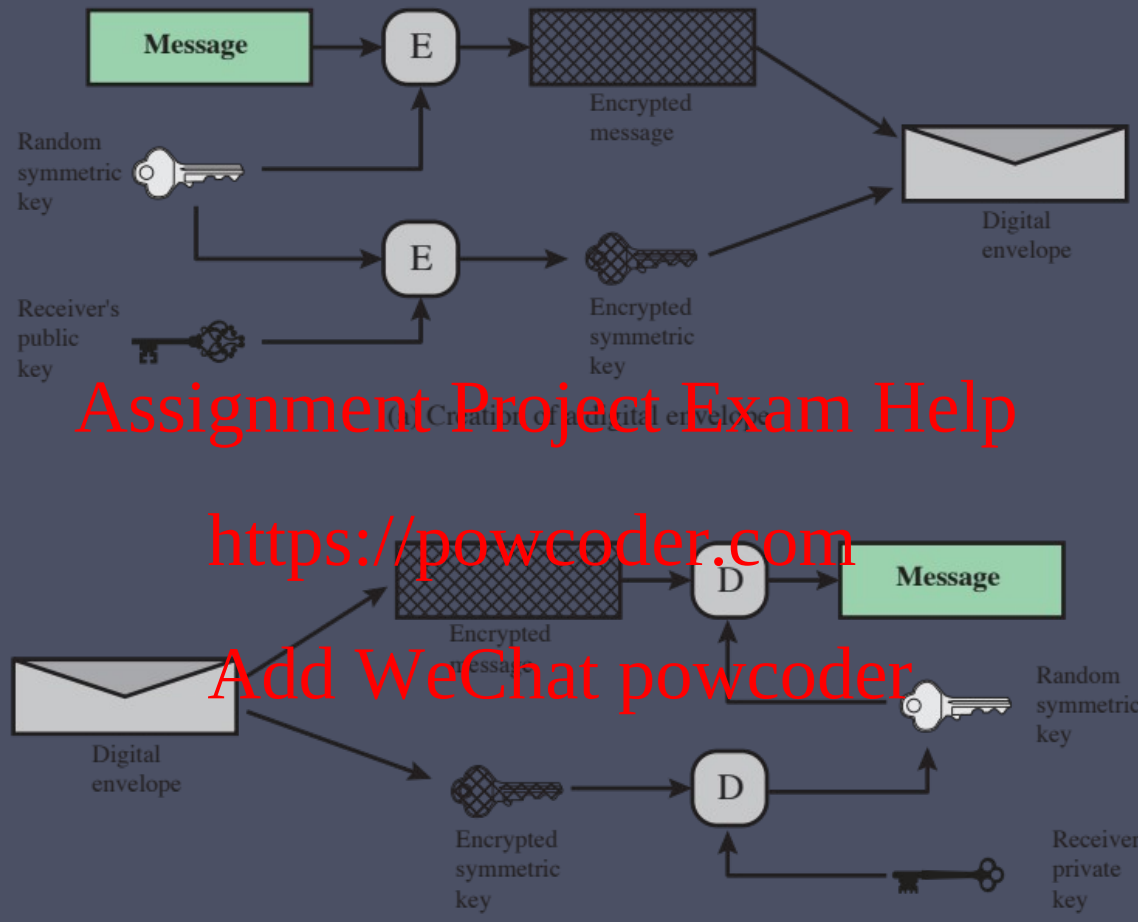


Figure 2.9 Digital Envelopes

Practical Application: Encryption of Stored Data

Common to encrypt transmitted data

Much less common for stored data

- There is often little protection beyond domain authentication and operating system access controls
- Data are archived for indefinite periods
- Even though erased, until disk sectors are reused data are recoverable

Approaches to encrypt stored data:

- Use a commercially available encryption package
- Back-end appliance
- Library based tape encryption
- Background laptop/PC data encryption

Elliptic Curve

- Proposed in 1985 by Neal Koblitz and Victor Miller
- Public key cryptography just like RSA
- User has two pairs of keys
- Discrete logarithm on elliptic curve is more difficult

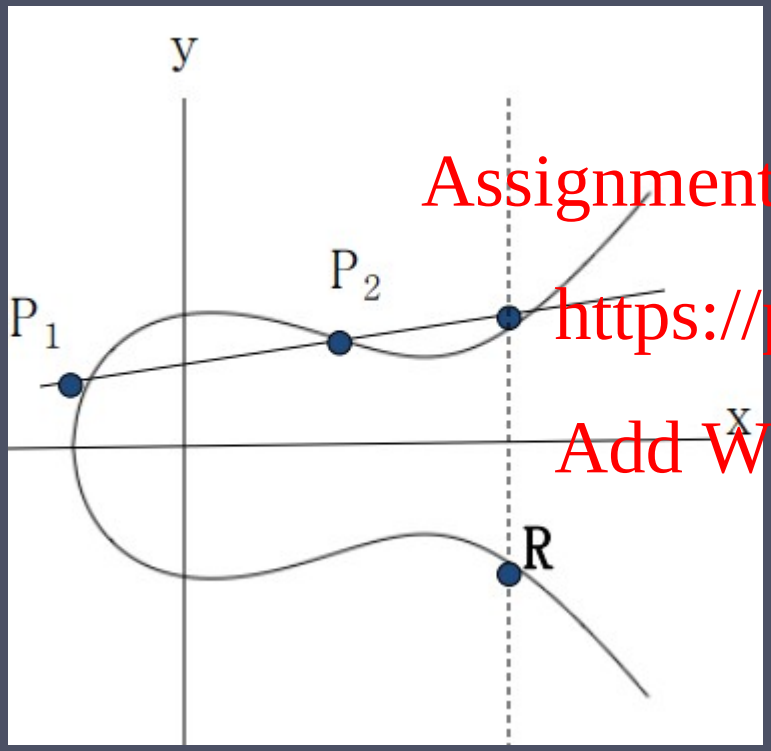
  y = mod p

  Challenge : Given y, g and p (g and p very large)

  it is not VERY EASY (impossible) to calculate x.

- All public-key cryptosystems have some underlying mathematical operation.
  - RSA has exponentiation (raising the message or ciphertext to the public or private values)
  - ECC has point multiplication (repeated addition of two points).

ELLIPTIC Curve



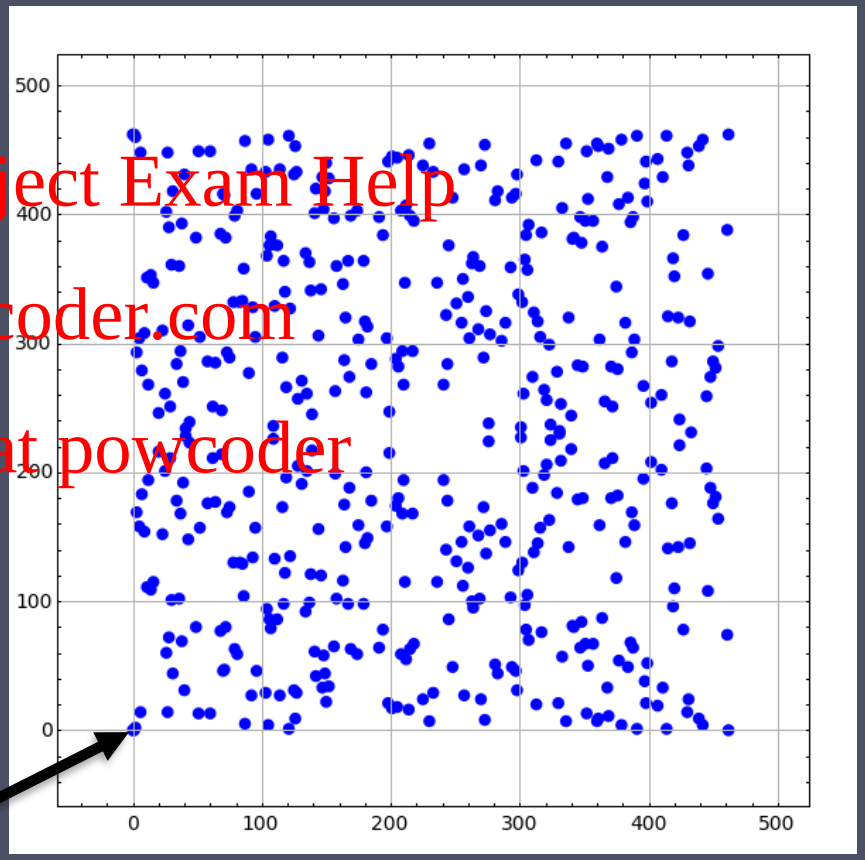
Consider elliptic curve
E : y 2 = x3 - x + 1

- if P1 and P2 are on E, we can define R = P1 + P2 as shown in picture
- Addition is all we need

Modulo arithmetic: cycle of numbers around, in ECC it use points

mod n was used in DH which used exponentiation

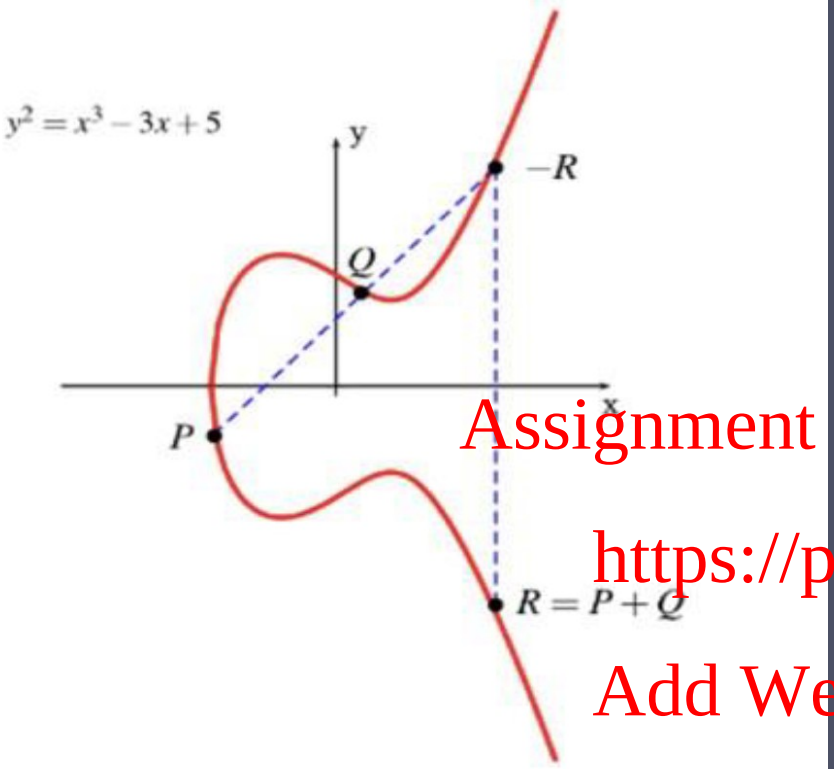
In ECC it is simply add a point to the, suppose g is our initial point, further points will be 2G, 3G, 4G….. These will be points somewhere on the curve

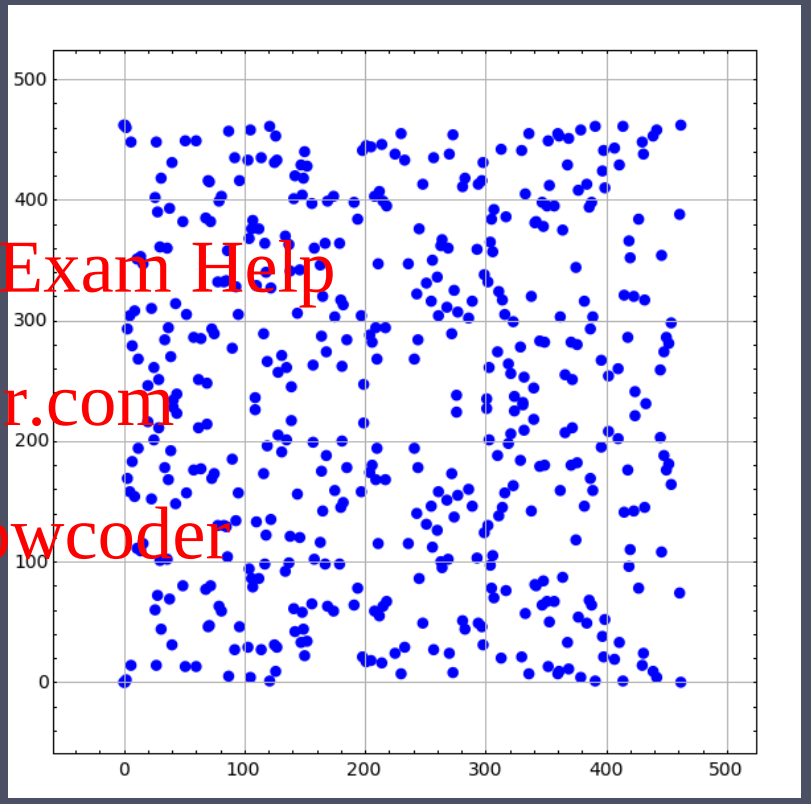


?G how many multiple points of g is this point

impossible to extract that information – private number

Elliptic Curve





Pick a point on the elliptic curve(G).

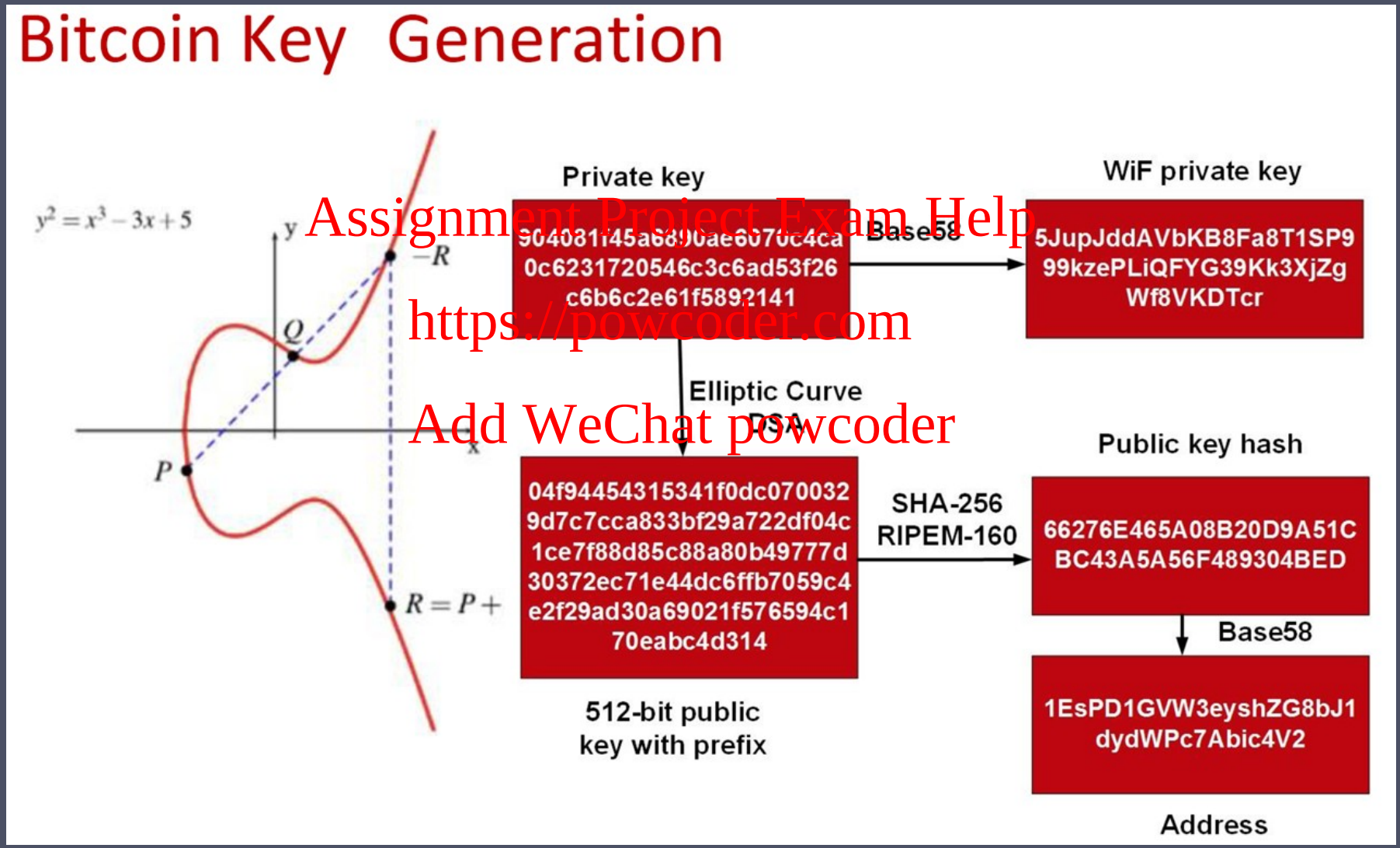
Generate a random number (n)

– this will be the private key.

Public key is P = n x G

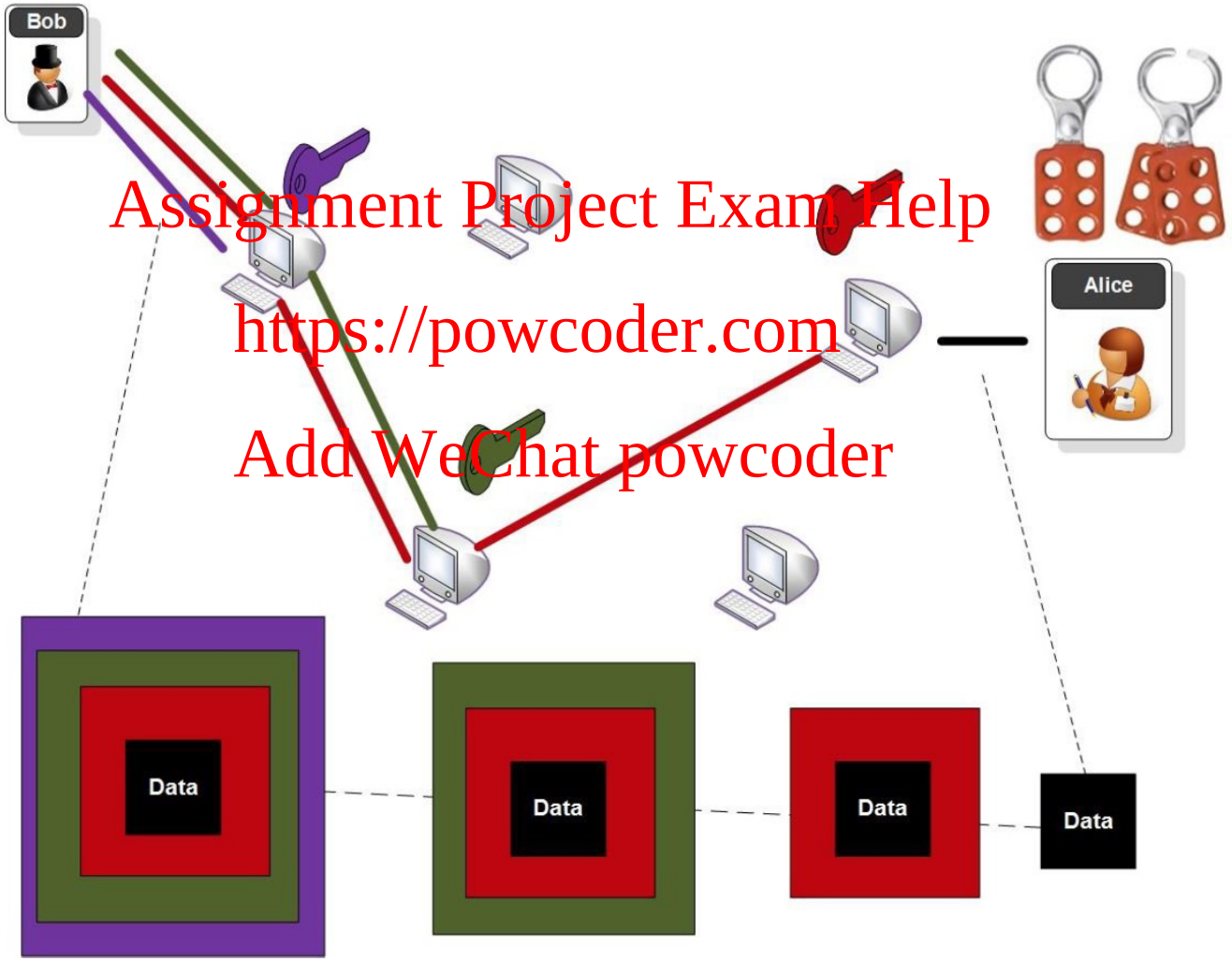
Bitcoin, IoT and Tor

Elliptic curve



Tor

Tor network use Elliptic curve



Applications

Wireless communication devices

– Smart cards

– Web servers that need to handle many encryption sessions

– Any application where security is needed but lacks the power, storage and computational power that is necessary for our current cryptosystems

- https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/