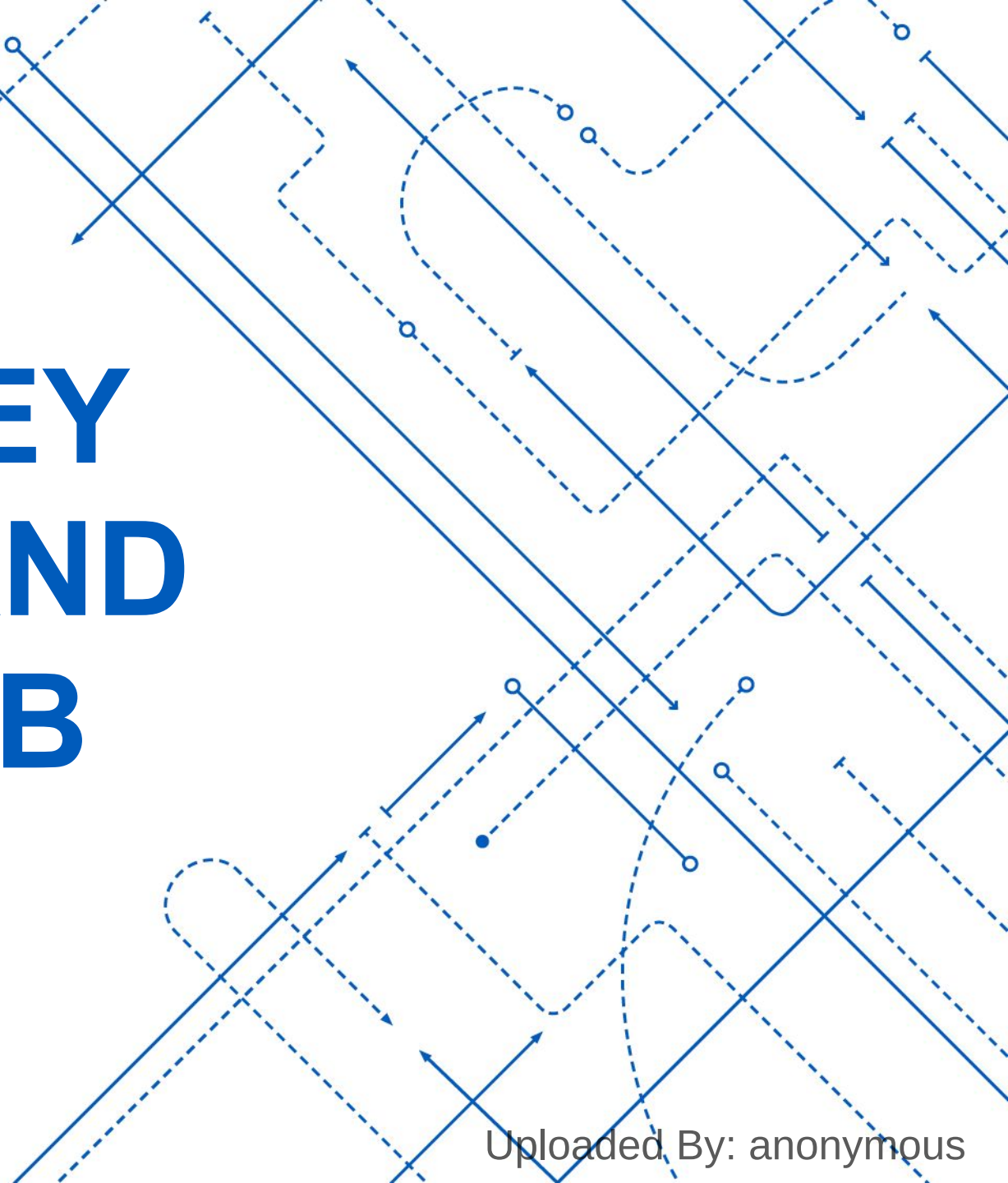
EXP #5

RSA PUBLIC-KEY ENCRYPTION AND SIGNATURE LAB

SLIDES BY: MOHAMAD BALAWI



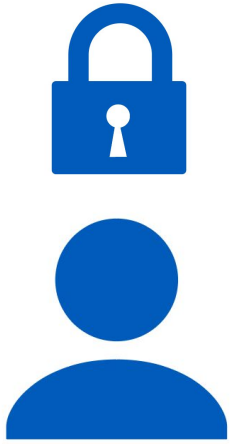
جامعة بيرزيت BIRZEIT UNIVERSITY

STUDENTS-HUB.com

Uploaded By: anonymous

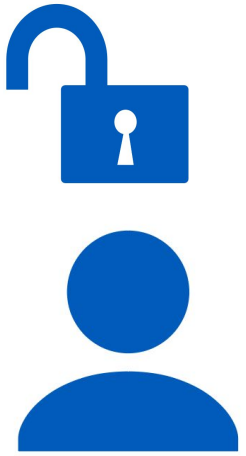
Secret Key Encryption

Secret Key Encryption uses a single shared key for both encryption and decryption, ensuring that only parties with the key can securely exchange messages.



Alice

But there is a fundamental issue in secret key encryption that prevents it from being used as an encryption standard.



Bob

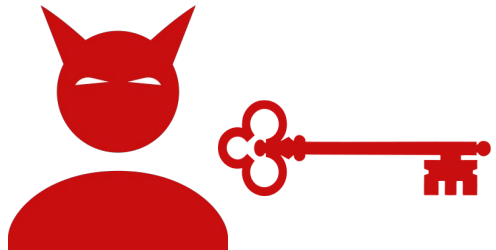
STUDENTS-HUB.com

Uploaded By: anonymous

Secret Key Encryption

The challenge is securely distributing and managing the shared secret key among communicating parties.

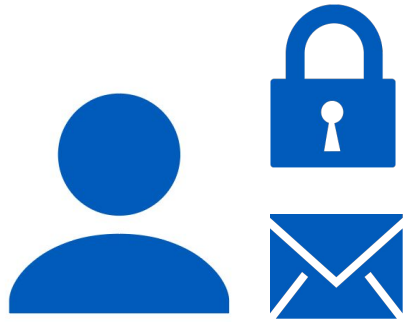
Consider a situation where Alice seeks to establish a secure connection with a local bank she hasn't interacted with previously. Since they lack a shared secret key, Alice's options are limited to either transmitting the key openly or visiting the bank and receiving assistance from a dedicated employee for this purpose.



STUDENTS-HUB.com
Uploaded By: anonymous

Public Key Encryption

Public key encryption solves the issue by using a pair of keys: a public key and a private key . The public key is freely distributed, allowing anyone to encrypt messages , while the private key remains secret and is used for decryption. This eliminates the need for sharing a secret key beforehand, enabling secure communication without prior contact or key exchange.



STUDENTS-HUB.com
Uploaded By: anonymous

Examples for SKE & PKE

PUBLIC KEY ENCRYPTION

Asymmetric scheme, has two keys, public one for encryption, and secret one for decryption.

- RSA (Rivest-Shamir-Adleman)
- Diffie-Hellman Key Exchange
- ElGamal
- Elliptic Curve Cryptography (ECC)

SECRET KEY ENCRYPTION

Symmetric scheme, has one key used for both encryption and decryption.

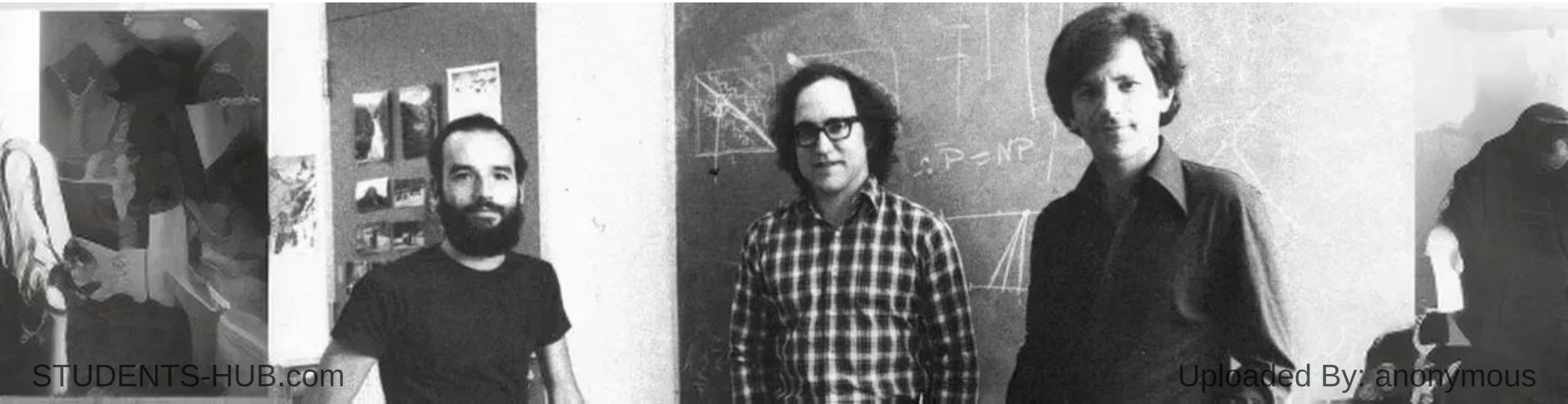
- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- 3DES (Triple Data Encryption Standard)
- Blowfish

STUDENTS-HUB.com

Uploaded By: anonymous

RSA (Rivest-Shamir-Adleman)

RSA is an asymmetric encryption algorithm that relies on the difficulty of prime factorization. It involves generating a public key and private key pair, where the public key is used for encryption and the private key is used for decryption.



STUDENTS-HUB.com Uploaded By: anonymous

RSA (How does it work?)

1. Choose two random large prime numbers. p, q
2. Multiply them to get the modulus n. $n = pq$
3. Calculate the totient of n. $\varphi(n) = (p-1)(q-1)$
4. Choose e such that $e = \begin{cases} 1 < e < \varphi(n) \\ \gcd(e, \varphi(n)) = 1 \end{cases}$
5. Determine d such that $ed \equiv 1 \pmod{\varphi(n)}$

   $d \equiv e^{-1} \pmod{\varphi(n)}$

STUDENTS-HUB.com Uploaded By: anonymous

RSA (How does it work?)

6. Announce the public key. (n, e)
7. Store the secret key. (n, d)
8. You can encrypt using: $c \equiv m^e \pmod{n}$
9. You can decrypt using: $m \equiv c^d \pmod{n}$

STUDENTS-HUB.com Uploaded By: anonymous

Digital Signature

Digital signatures, used in asymmetric encryption like RSA, ensure data integrity and non-repudiation. In contrast, MACs are employed in symmetric encryption for message authentication.

Unlike the encryption process, we sign the message using the secret key, and that is how we ensure a unique signature, and since everyone knows the public key, they can use it to verify the signature.

- Generate a signature using secret key. $s = m^d \pmod n$
- Verify the signature using the public key. $m = s^e \pmod n$

STUDENTS-HUB.com Uploaded By: anonymous

X.509 Certificate

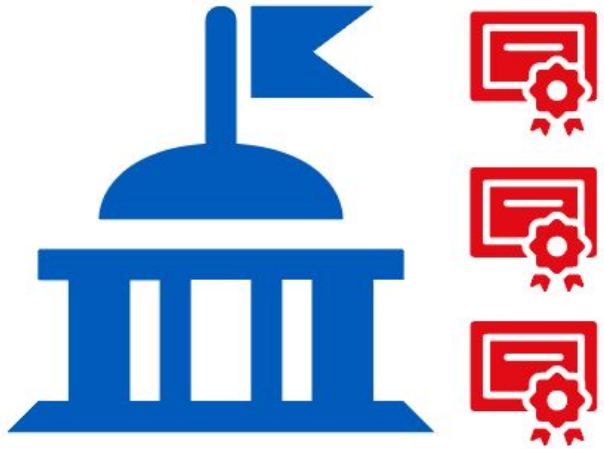
X.509 is an International Telecommunication Union (ITU) standard defining the format of public key certificates, it is used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS. It includes important info such as:

- **Subject**: Identifies the entity the certificate is issued to.
- **Issuer**: Identifies the entity that issued the certificate.
- **Validity Period**: consisting of a start date and an expiration date.
- **Public Key**: Includes the public key of the subject.
- **Signature Value**: Contains the digital signature generated by the issuer's private key to verify the integrity and authenticity of the certificate.

STUDENTS-HUB.com Uploaded By: anonymous

Certificate Authority

A Certificate Authority (CA) is a trusted entity responsible for issuing digital certificates used to verify the authenticity and identity of individuals, organizations, or websites on the internet. CAs validate the information provided by the certificate requester and digitally sign the certificate to attest to its legitimacy.

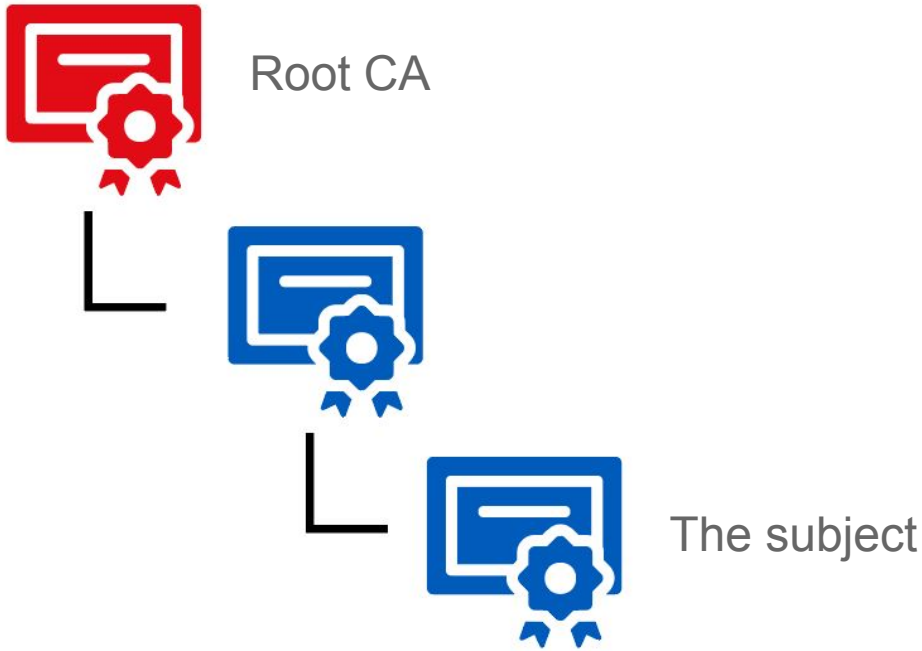


STUDENTS-HUB.com

Uploaded By: anonymous

Chain of Trust

A chain of trust is a hierarchy of certificates where trust is delegated from higher-level authorities down to lower-level entities. Each certificate in the chain validates the authenticity of the next one, ensuring secure communication and authentication.



STUDENTS-HUB.com
Uploaded By: anonymous

BIGNUM APIs

BIGNUM APIs in C are necessary for handling large integers that exceed the range of built-in data types like int or long. These APIs provide functions and structures for performing arithmetic operations, such as addition, subtraction, multiplication, and division, on arbitrarily large numbers. This capability is crucial for cryptographic algorithms, mathematical computations, and other applications where precision and size are significant factors.

Largest datatype in C is **long long int** (64-bit).

STUDENTS-HUB.com

Uploaded By: anonymous