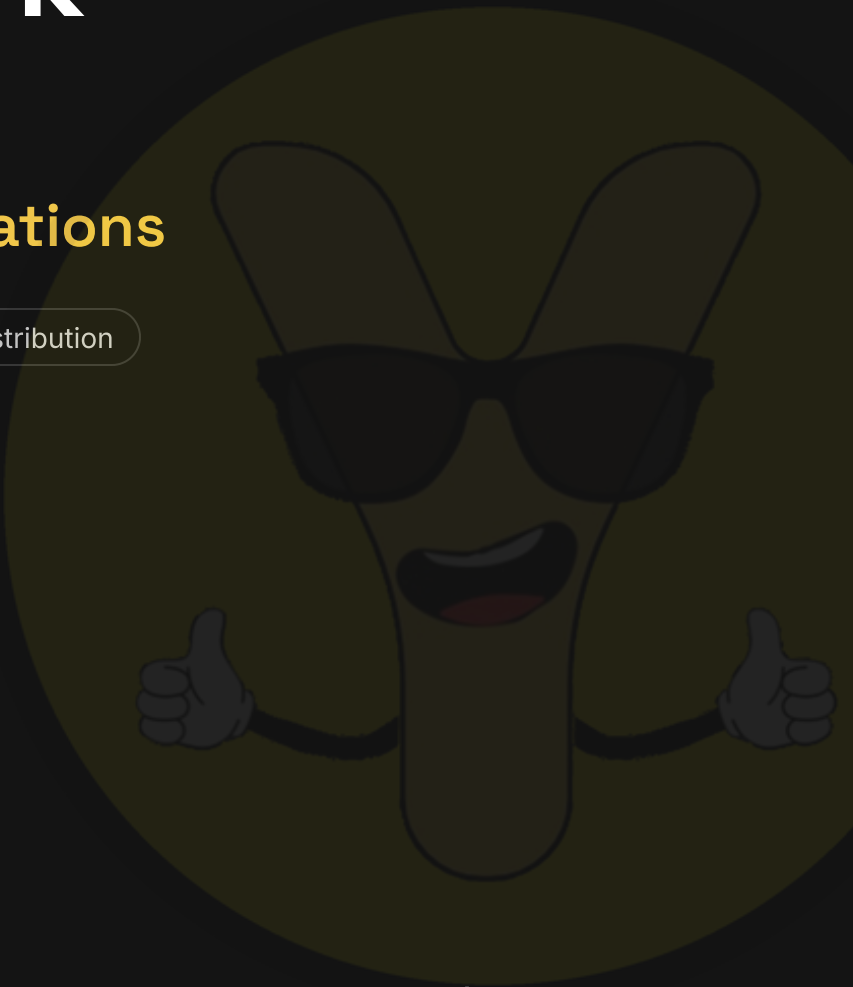
AKTU · 4TH YEAR · SEMESTER 7 · BCS072

Cryptography and Network Security

Unit 4 — Key Management and Authentication Applications

- Key Management and distribution: Symmetric key distribution
- Diffie-Hellman Key Exchange
- Public key distribution
- X.509 Certificates
- Public key Infrastructure
- Authentication Applications: Kerberos
- Electronic mail security: pretty good privacy (PGP)
- S/MIME



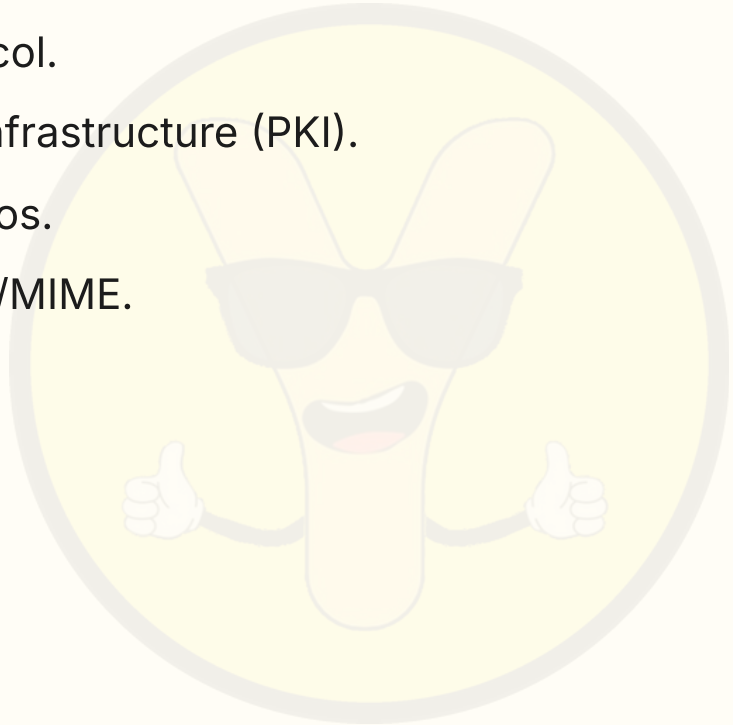
DECODED BY

Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

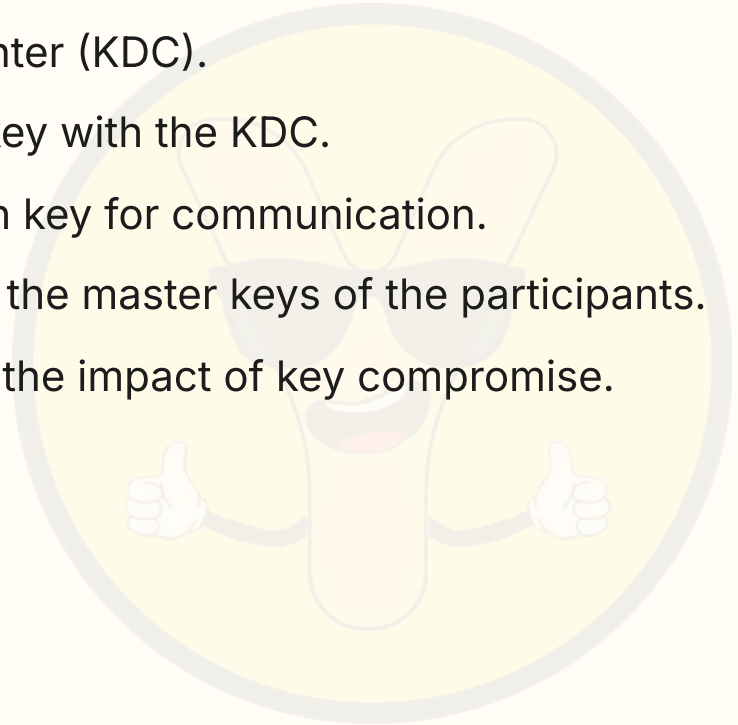
Unit 4: Key Management and Authentication

- Key Management: Symmetric and Public key distribution methods.
- Diffie-Hellman Key Exchange protocol.
- X.509 Certificates and Public Key Infrastructure (PKI).
- Authentication Applications: Kerberos.
- Electronic Mail Security: PGP and S/MIME.

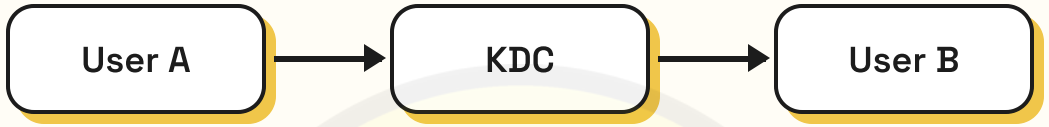


Symmetric Key Distribution

- Problem: How to share a secret key securely between two parties.
- Solution: Use a Key Distribution Center (KDC).
- Each user shares a unique master key with the KDC.
- KDC generates a temporary session key for communication.
- The session key is encrypted using the master keys of the participants.
- Ensures forward secrecy and limits the impact of key compromise.



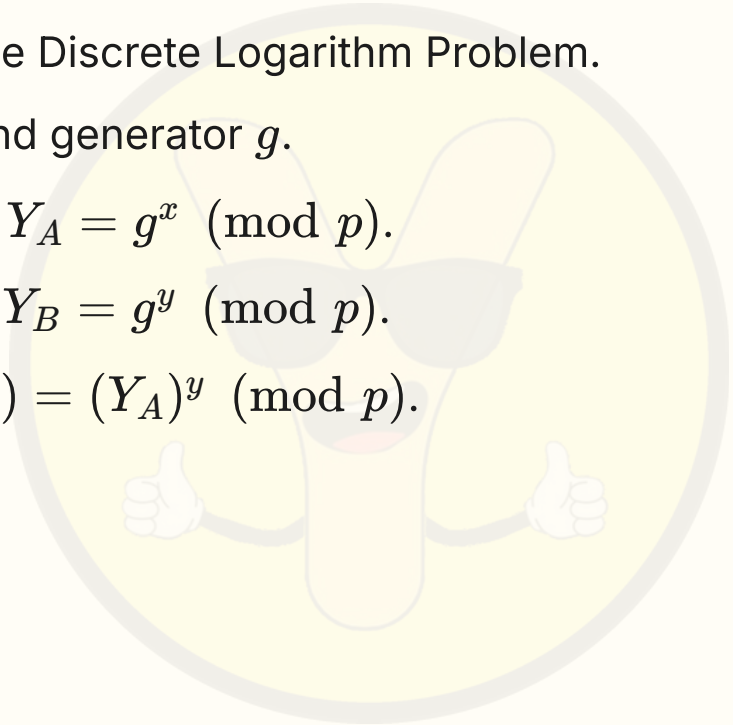
Symmetric Key Distribution Flow



A requests session key, KDC provides encrypted key to A and B.

Diffie-Hellman Key Exchange

- Purpose: Establish a shared secret over an insecure channel.
- Security relies on the difficulty of the Discrete Logarithm Problem.
- Public parameters: Large prime p and generator g.
- User A selects private key x, sends $Y_A = g^x \pmod{p}$.
- User B selects private key y, sends $Y_B = g^y \pmod{p}$.
- Shared secret $K = (Y_B)^x \pmod{p} = (Y_A)^y \pmod{p}$.



Diffie-Hellman Example

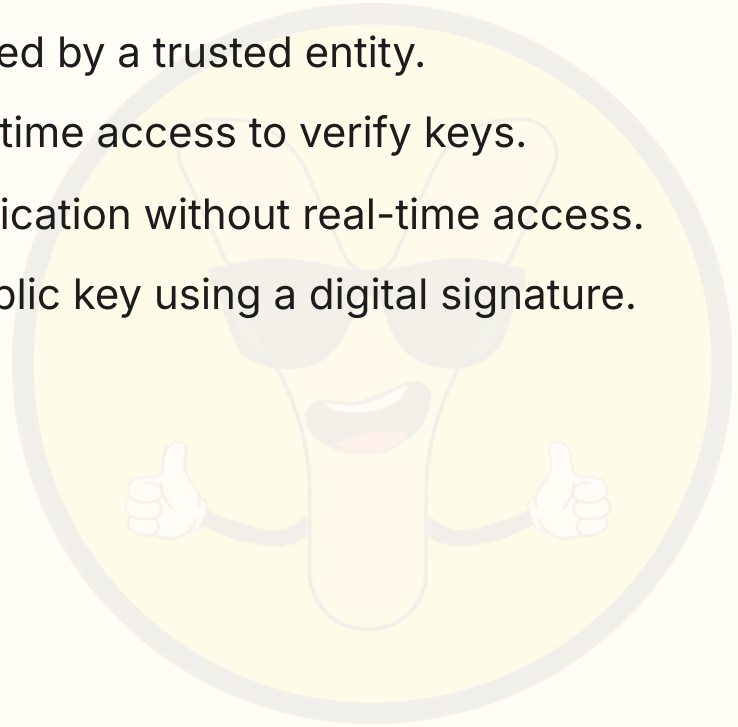
Given $p = 11, g = 2$. A chooses $x = 6$, B chooses $y = 9$. Find shared secret.

1. A computes $Y_A = 2^6 \pmod{11} = 64 \pmod{11} = 9$.
2. B computes $Y_B = 2^9 \pmod{11} = 512 \pmod{11} = 6$.
3. A computes $K = (Y_B)^x \pmod{11} = 6^6 \pmod{11} = 46656 \pmod{11} = 3$.
4. B computes $K = (Y_A)^y \pmod{11} = 9^9 \pmod{11} = 3$.

Shared secret key K = 3.

Public Key Distribution

- Public Announcement: Users broadcast keys (vulnerable to impersonation).
- Publicly Available Directory: Managed by a trusted entity.
- Public Key Authority: Requires real-time access to verify keys.
- Public Key Certificates: Allows verification without real-time access.
- Certificates bind an identity to a public key using a digital signature.



X.509 Certificates

X.509

A standard format for public key certificates used in PKI.

- Contains: Version, Serial Number, Signature Algorithm, Issuer, Validity Period, Subject, Subject Public Key Info.
- Signed by a Certificate Authority (CA).
- Allows users to verify the authenticity of a public key.

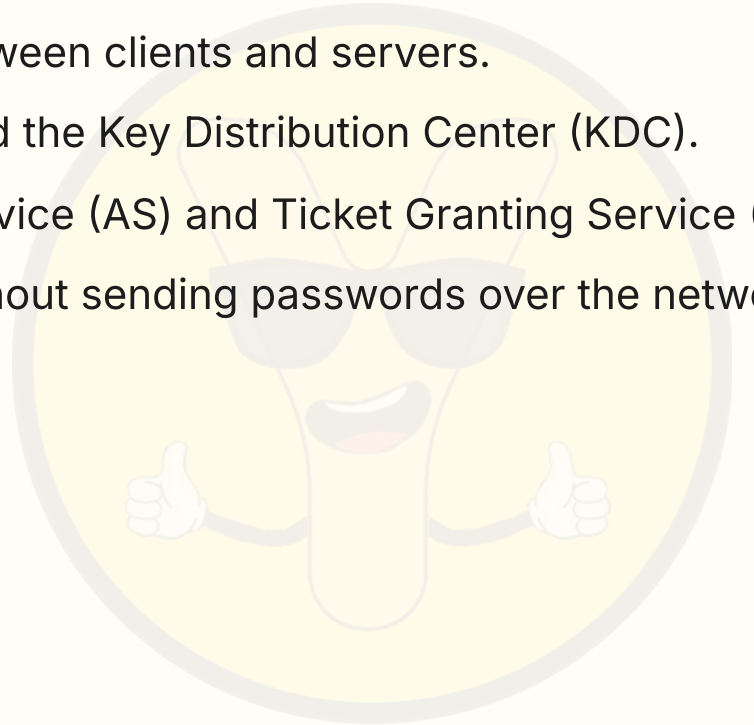
Public Key Infrastructure (PKI)

- Definition: Set of roles, policies, and procedures to manage digital certificates.
- Components: Certificate Authority (CA), Registration Authority (RA), Repository, End Entity.
- CA: Issues and revokes certificates.
- RA: Verifies identity of certificate applicants.
- Repository: Stores certificates and Certificate Revocation Lists (CRL).

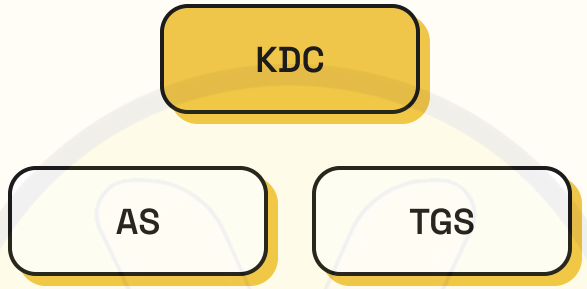


Kerberos

- Definition: A network authentication protocol based on symmetric cryptography.
- Provides mutual authentication between clients and servers.
- Relies on a trusted third party called the Key Distribution Center (KDC).
- KDC consists of Authentication Service (AS) and Ticket Granting Service (TGS).
- Uses 'Tickets' to prove identity without sending passwords over the network.



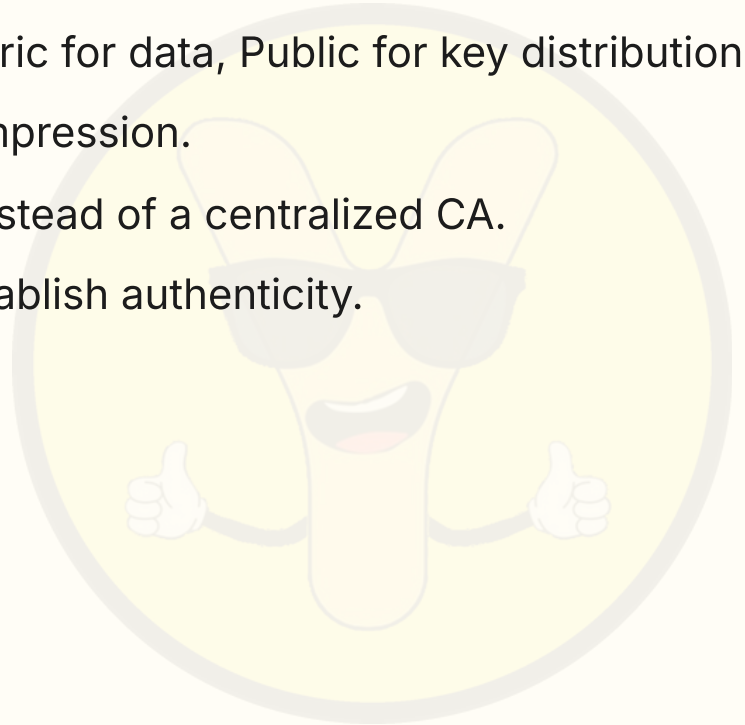
Kerberos Architecture



KDC manages authentication and ticket granting.

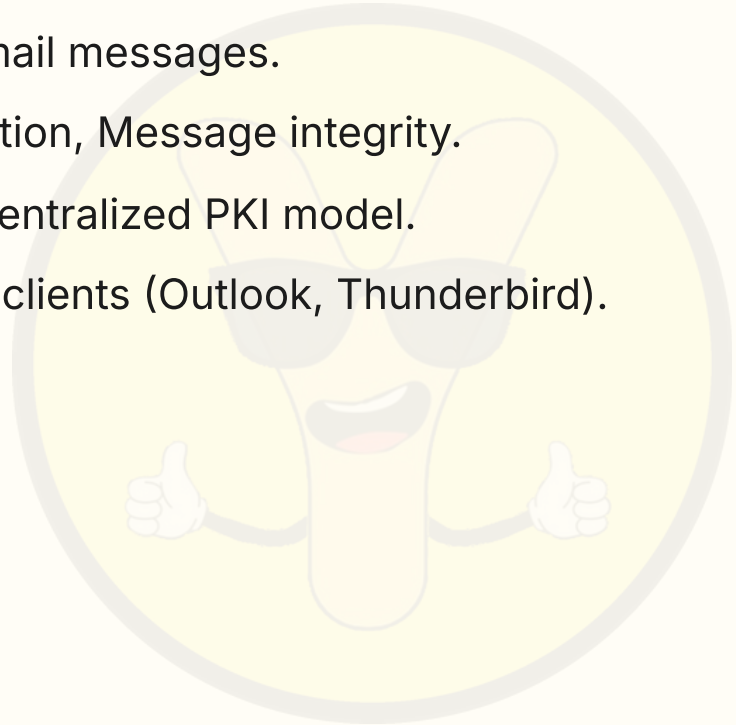
Electronic Mail Security: PGP

- Pretty Good Privacy (PGP) provides confidentiality and authentication.
- Uses hybrid cryptography: Symmetric for data, Public for key distribution.
- Supports digital signatures and compression.
- PGP uses a 'Web of Trust' model instead of a centralized CA.
- Users sign each other's keys to establish authenticity.



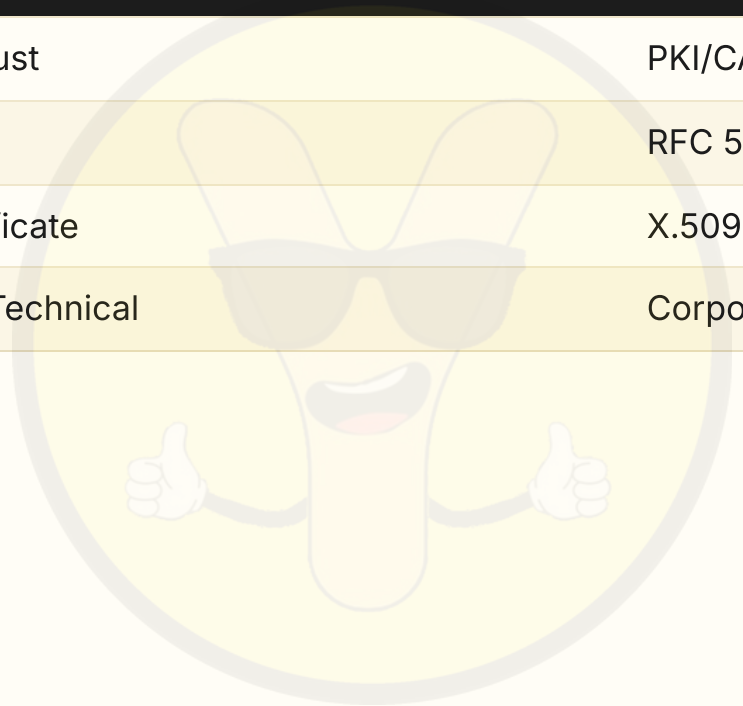
S/MIME

- Secure/Multipurpose Internet Mail Extensions.
- Adds security to MIME-encoded email messages.
- Provides: Digital signatures, Encryption, Message integrity.
- Relies on X.509 certificates and a centralized PKI model.
- Widely supported by modern email clients (Outlook, Thunderbird).



PGP vs S/MIME

Feature	PGP	S/MIME
Trust Model	Web of Trust	PKI/CA
Standard	RFC 4880	RFC 5751
Certificate	PGP Certificate	X.509
Usage	Personal/Technical	Corporate/Enterprise



Exam corner

- **Q1** Explain the role of a KDC in symmetric key distribution.
- **Q2** Derive the Diffie-Hellman key exchange protocol with steps.
- **Q3** What are the contents of an X.509 certificate?
- **Q4** Describe the components and working of Kerberos.
- **Q5** Differentiate between PGP and S/MIME.
- **Q6** Explain the architecture of a Public Key Infrastructure (PKI).
- **Q7** Why is the Discrete Logarithm Problem crucial for Diffie-Hellman?

Unit 4 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 5 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

