➔ What is a digital signature?

- A **mathematical technique** used to validate the authenticity and integrity of a digital document, message or software.
- It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security.
- Intended to solve the problem of tampering and impersonation in digital communications.
- Can provide evidence of **origin, identity** and **status** of electronic documents, transactions and digital messages.

➔ How do digital signatures work?

- Based on public key cryptography, also known as **asymmetric cryptography**.
- Using a **public key algorithm**, such as **Rivest-Shamir-Adleman (RSA)**, two keys are generated, creating a mathematically linked pair of keys: one private and one public.
- Digital signatures work through public key cryptography's two mutually authenticating cryptographic keys.

➔ What are the benefits of digital signatures?

- **Security:**
  - Ensure a legal document isn't altered and signatures are legitimate.
- **Timestamping:**
  - Provides the date and time of a digital signature and is useful when timing is critical, such as for stock trades, lottery ticket issuance and legal proceedings
- **Time savings:**
  - Simplify the time-consuming processes of physical document signing, storage and exchange, letting businesses quickly access and sign documents.
- **Cost savings:**
  - Organizations can go paperless by saving money on physical resources, time, personnel and office space used to manage and

transport documents.

➔ What are the challenges of digital signatures?

- **Insecure channels:** Channels used to transmit documents can still have inadequate security measures. Without proper encryption and authentication, they could lead to compromised documents and data loss.
- **Key management:** Compromised or lost keys are useless; therefore, organizations must be prepared to craft policies and procedures for employees to properly manage their keys, which can be complicated.
- **Compliance:** Different standards are used in different jurisdictions regarding digital signatures, so an organization must consult with legal experts or have a knowledgeable person to handle these matters.

➢ Case Studies

○ Indian Bank Fraud Case Study

■ Introduction

- On **July 16, 2024**, a **Noida**-based bank in India fell victim to a significant cyber heist, resulting in a loss of **₹16.71 crore** (US$2.1 million)
- The attack involved a sophisticated **Fund Transfer Fraud (FTF)** where hackers compromised the bank's security systems, transferring the stolen funds to **84 different accounts**.

■ The Attack: How It Happened

- The cyberattack unfolded on July 16, 2024, when hackers infiltrated the bank's systems, likely through compromised login credentials and exploited server vulnerabilities.
- Breach went undetected until a routine check by the **bank's IT manager** revealed a **₹3.60 crore** discrepancy in the **Real-Time Gross Settlement (RTGS)** account balance sheets.
- Further investigation uncovered that **₹16.71 crore** had been illicitly transferred to **84 accounts** across various locations.
- The breach raised concerns about potential compromise of sensitive customer data.

■ The Impact: Financial and Operational Disruption

- The bank lost **₹16.71 crore**, severely impacting its financial stability.
- The bank had to halt certain operations to investigate and contain the breach, disrupting normal activities.
- The potential exposure of sensitive customer data posed additional risks, including legal liabilities and loss of customer trust.
-

○