

Secure Operating Systems (CYB610)

Master of Science in Cybersecurity

Lecture 8: Biometrics and Database Security

Dr. Ibrahim Gomaa

*Faculty of Informatics
Midocean University*



Chapter

08

Topics

This chapter covers the following topics and concepts:

- **Biometrics**
- **Authentication in distributed systems**
- **Databases Security**
- **Protecting sensitive data**
- **Data mining and big data**

Chapter

08

Goals

When you complete this chapter, you will be able to:

- **Describe why we use biometrics**
- **Explain the phases of biometric system**
- **Describe the authentication in distributed systems**
- **Explain the token-based authentication**



- Use a person's physical characteristics
 - fingerprint, voice, face, keyboard timing, ...
- Advantages
 - Cannot be disclosed, lost, forgotten
- Disadvantages
 - Cost, installation, maintenance
 - Reliability of comparison algorithms
 - False positive: Allow access to unauthorized person
 - False negative: Disallow access to authorized person
 - Privacy?
 - If forged, how do you revoke?





➤ **A biometric should be**

- **Universal:** The ideal biometric should apply to virtually everyone.
- **Distinguishing:** The ideal biometric should distinguish with virtual certainty.
- **Permanent:** The physical characteristic being measured should never change.
- **Collectible:** The physical characteristic should be easy to collect without any potential to cause harm to the subject.
- **Reliable, robust, and user-friendly**



- Biometrics are very reliable for **Identification** but much less effective for **authentication**
- The difference is between a system that looks at a hand geometry and says "this is Captain Hook" (**identification**) versus a man who says "I am, Captain Hook, presenting my hand to prove who I am" and the system confirms "this hand matches Captain Hook's template" (**authentication**).



❖ Identification:

- Identify the subject from a list of many possible subjects.
- E.g., a suspicious fingerprint from a crime scene is sent to the FBI fingerprint database for comparison with all records on file. In this case, the comparison is one to many.

❖ Authentication:

- The comparison is one to one
- E.g., if someone claiming to be Alice uses a thumbprint mouse biometric, the captured thumbprint image is only compared with the stored thumbprint of Alice.



- More secure replacement for passwords
- Cheap and reliable biometrics needed
 - An active area of research
- Biometrics used in security are :
 - Thumbprint mouse
 - Palm print for secure entry
 - Fingerprint to unlock car door, etc.
- But biometrics not too popular
 - Has not lived up to its promise (yet?)



- Biometric recognition devices are costly
- All biometric readers use **sampling** and establish a **threshold** for when a match is close enough to **accept**.
- Biometrics can become a single point of failure.
- Although equipment is improving, there are still **false readings**
- The speed at which a recognition must be done **limits accuracy**.
- Although we like to think of biometrics as unique parts of an individual, forgeries are possible.



➤ Common uses

❑ Specialized situations, physical security Combine :

- Multiple biometrics
- Biometric and PIN
- Biometric and token





❖ The Enrollment Phase:

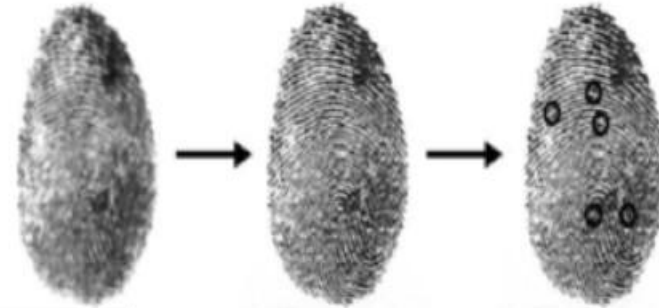
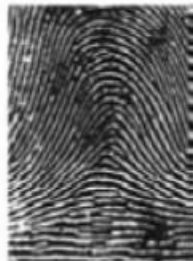
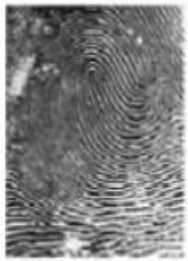
- subjects have their biometric information entered into a database.

❖ The Recognition Phase:

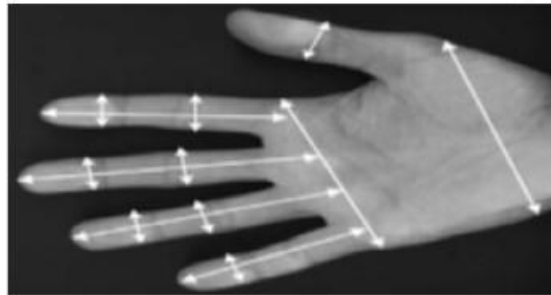
- subjects have their biometric information compared with that stored in the database.



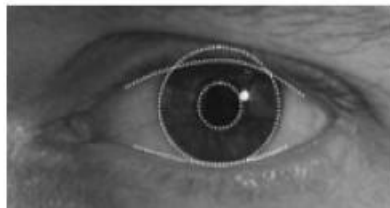
- Fingerprints



- Hand Geometry



- Iris Scan

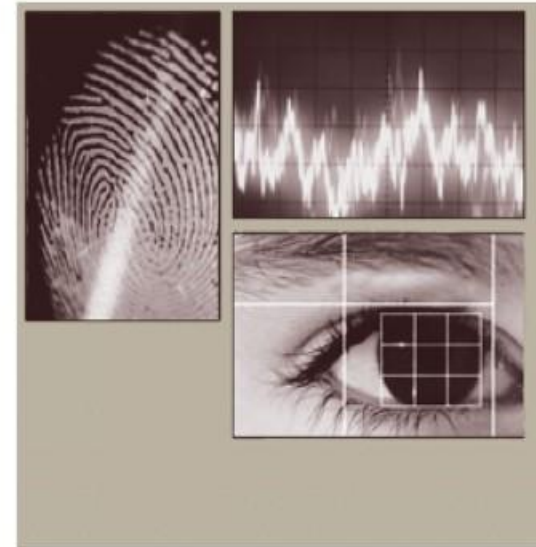




- For fingerprint biometric systems, the error rate is about 5%
- hand geometry has an equal error rate of about 10^{-3}



- Biometrics are biological authenticators, based on some physical characteristics of the human body.
- Now there are devices to recognize the following biometrics:
 - fingerprints
 - hand geometry (shape and size of fingers)
 - retina and iris (parts of the eye)
 - voice
 - handwriting
 - blood vessels in the finger
 - face.





❖ Authentication with biometrics has advantages over passwords because:

- a biometric cannot be:
 - lost,
 - stolen,
 - forgotten,
 - lent,
 - or forged and is
- always available,
- always at hand.



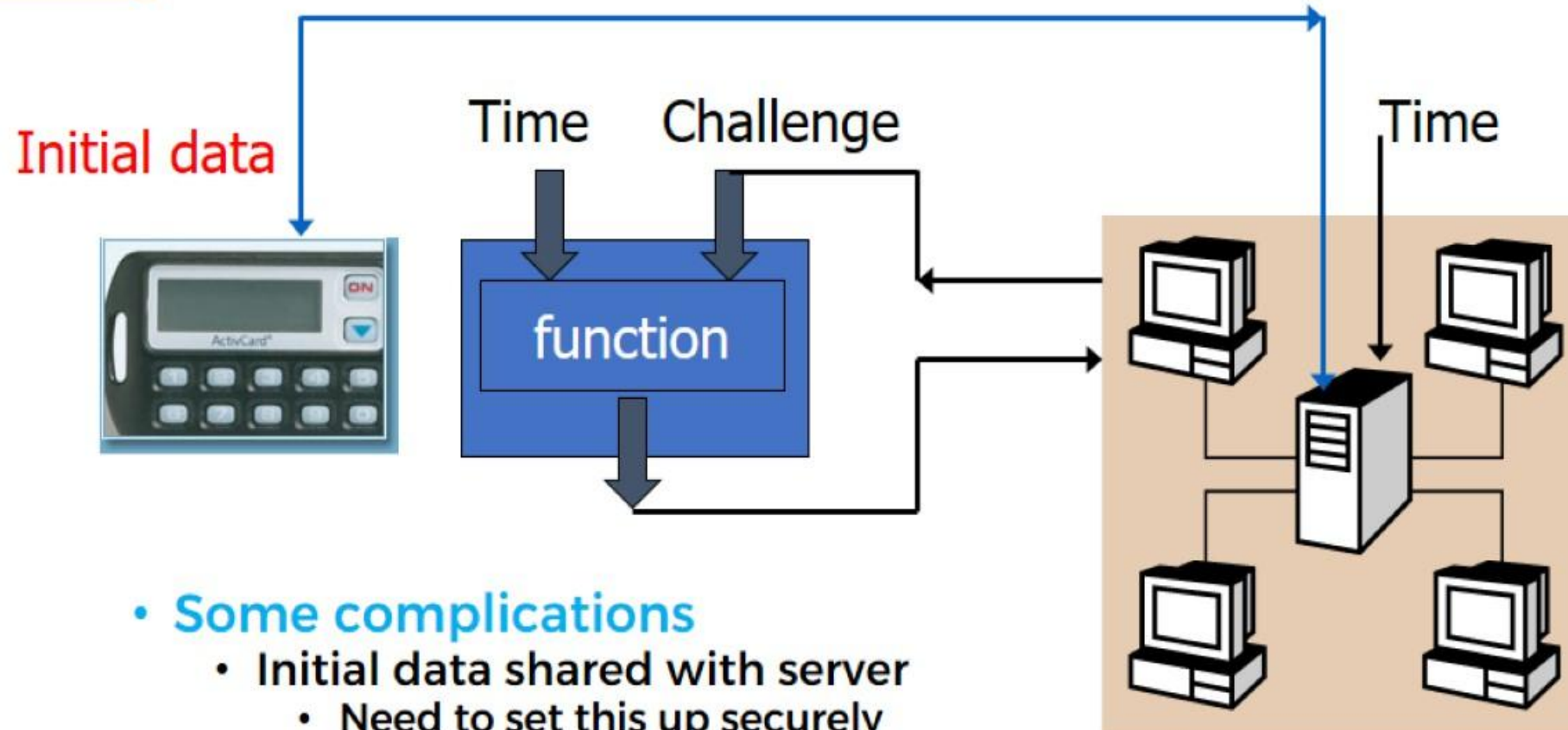
- Single sign-on, Microsoft Passport
- Trusted Intermediaries



❖ Smart Card

- With embedded CPU and memory
 - Carries conversation with a small card reader
- Various forms
 - PIN protected memory card
 - Enter PIN to get the password
 - Cryptographic challenge/response cards
 - A cryptographic key in memory
 - Computer create a random challenge
 - Enter PIN to encrypt/decrypt the challenge with the card
 - Cryptographic Calculator (readerless smart card)
 - Simulating a smartcard: user enter the encrypted result





- **Some complications**
 - Initial data shared with server
 - Need to set this up securely
 - Shared database for many sites
 - Clock skew



- Launched 1999
 - Claim > 200 million accounts in 2002
 - Over 3.5 billion authentications each month
- Microsoft Passport is a two-factor authentication (2FA) system that combines a PIN or biometrics (via Windows Hello) with encrypted keys from a user's device to provide two-factor authentication.
 - If you sign into Windows with fingerprint or face recognition, then you are already using Windows Hello.
- What does Microsoft Passport service do?
 - It allows you to log in to Windows using your Active Directory and replace passwords, smartcards, and virtual smart cards.



- **How do I get a Microsoft Passport?**

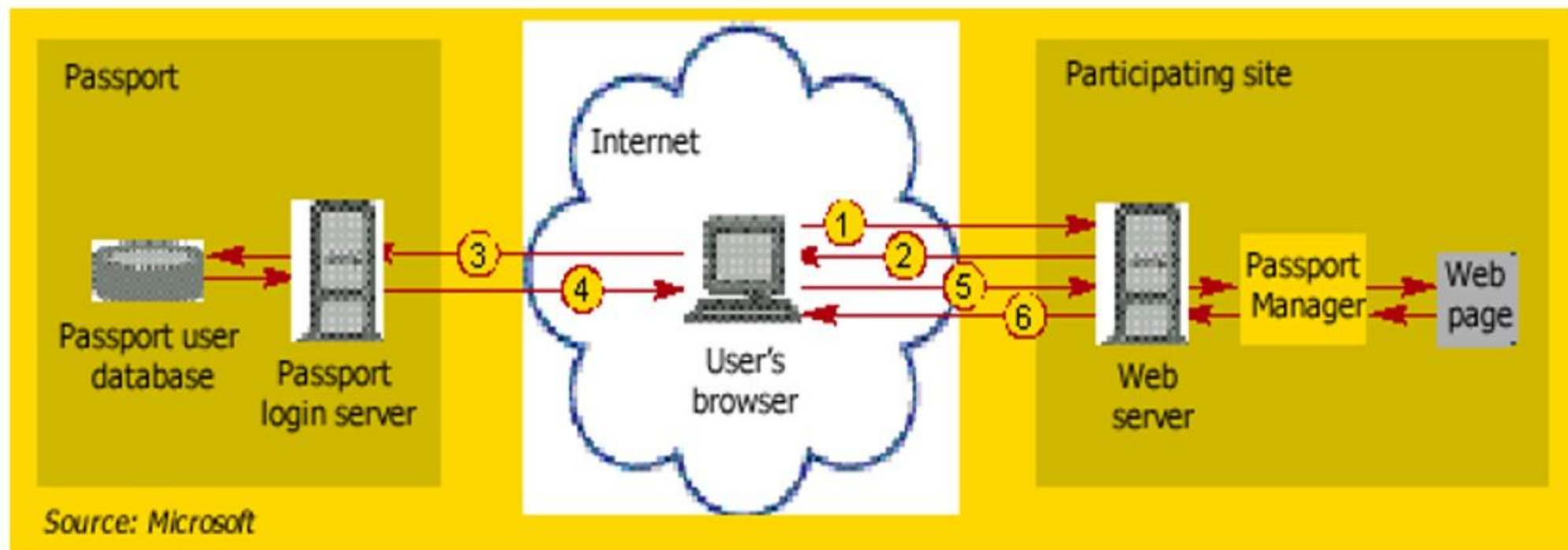
Creating Passport: Upon first login to their device the user is prompted to create a gesture. After they create the gesture, Windows creates a private-public key pair and registers the user's public key while the private key is protected by encrypted with a locally derived secret.



❖ Log in to many websites using one account

- Used by MS services Hotmail, MSN Messenger or MSN subscriptions; also Radio Shack, etc.
- Hotmail or MSN users automatically have Microsoft Passport accounts set up

❖ The Passport may continue to evolve; bugs have been uncovered



Sign-In of the Times. 1) The Passport authentication process begins when a user signs in from a participating Web site. 2) The user's browser is redirected to a Passport login server. 3) The Passport server prompts the user for an e-mail address and password and checks it against its database. 4) The Passport server places three encrypted cookies to the user's browser, which is redirected to the participating Web site. 5) The participating site decrypts the authentication cookie via the Passport Manager object. 6) The site serves up the requested Web page.



Symmetric key problem:

- How do two entities establish a shared secret key over the network?

Solution:

- trusted key distribution center (KDC) acting as intermediary between entities

Public key problem:

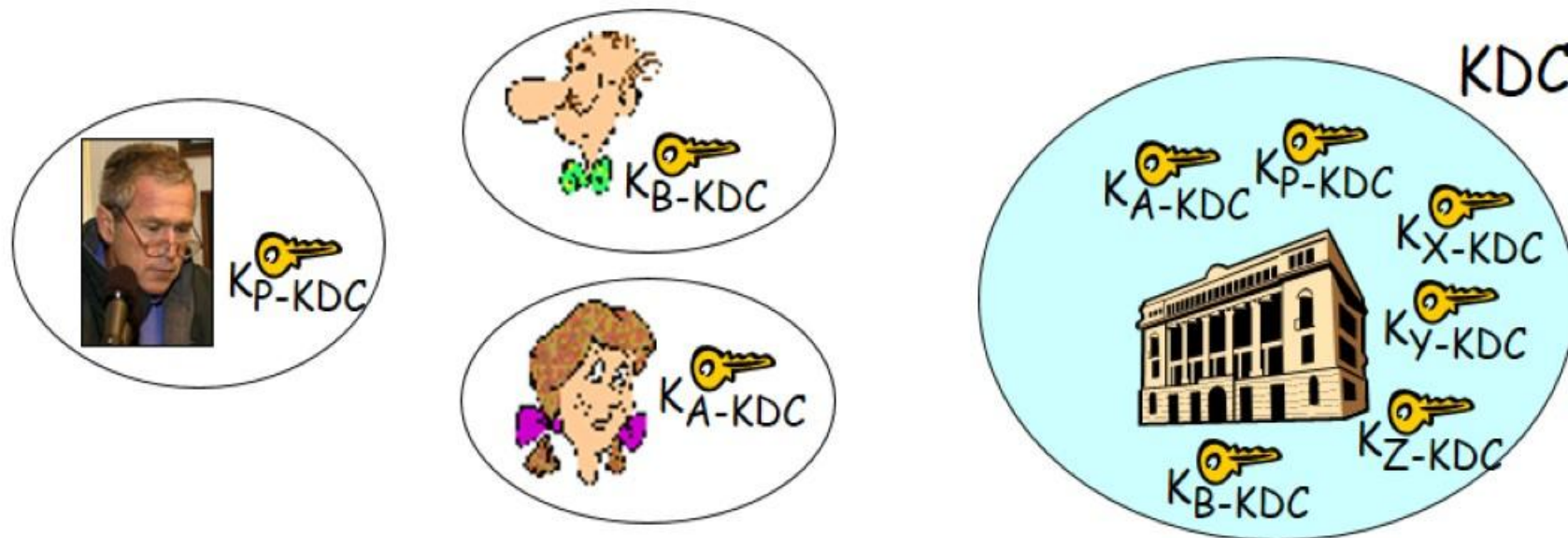
- When Alice obtains Bob's public key (from web site, e-mail, flash memory), how does she know it is Bob's public key, not a spy?

Solution:

- trusted certification authority (CA)

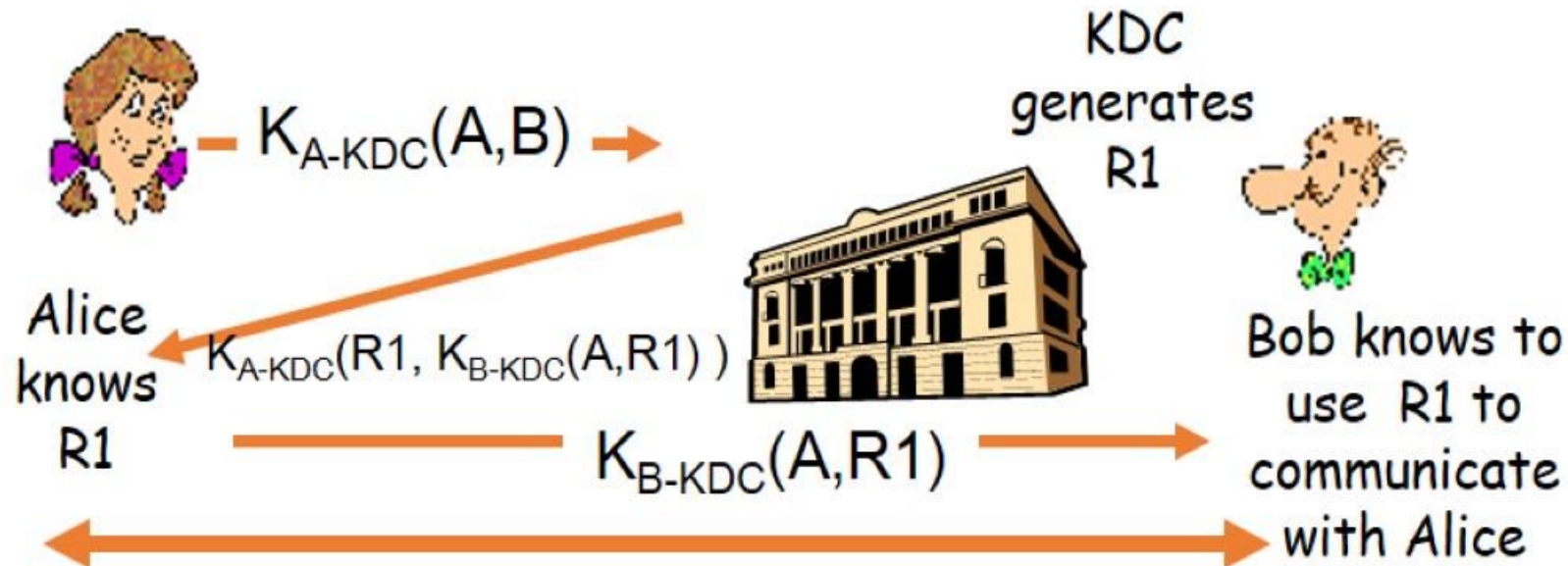


- Alice, Bob need shared symmetric key.
- **KDC:** server shares a different secret key with *each* registered user (many users)
- Alice, Bob know own symmetric keys, K_{A-KDC} K_{B-KDC} , for communicating with KDC.





Q: How does KDC allow Bob, Alice to determine shared symmetric secret key to communicate with each other?



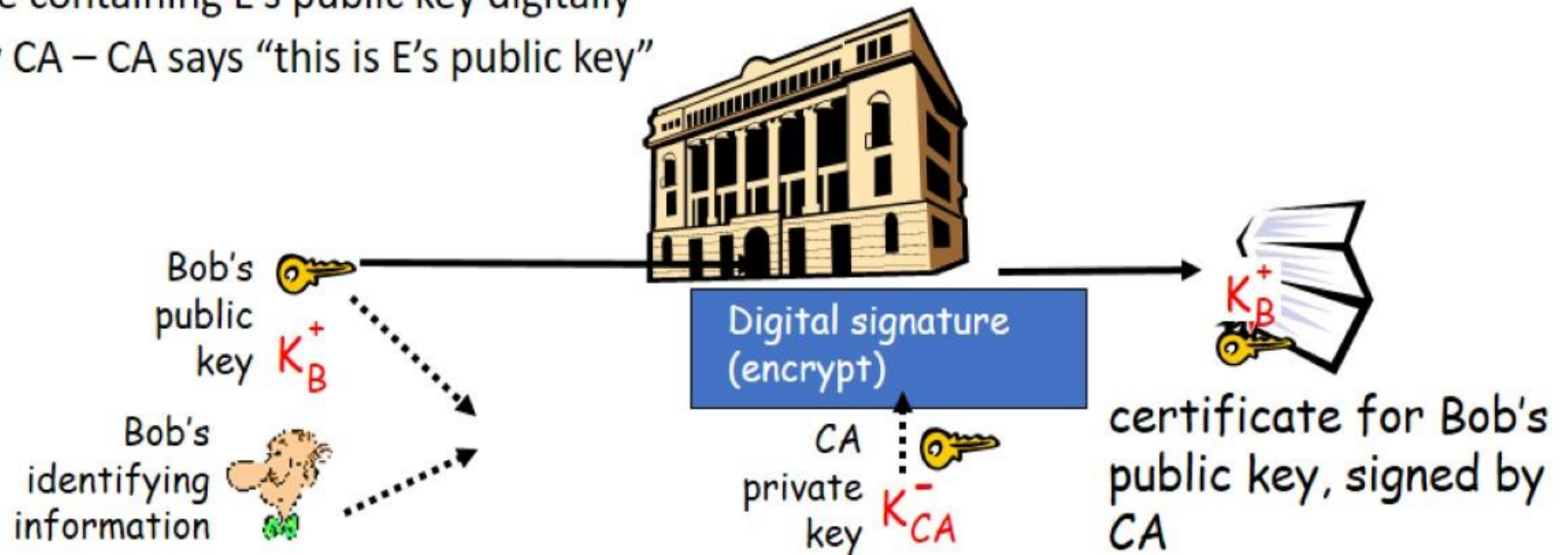
Alice and Bob communicate: using $R1$ as *session key* for shared symmetric encryption



- In $K_{A-KDC}(R1, K_{B-KDC}(A, R1))$, the $K_{B-KDC}(A, R1)$ is also known as a ticket
- Comes with expiration time

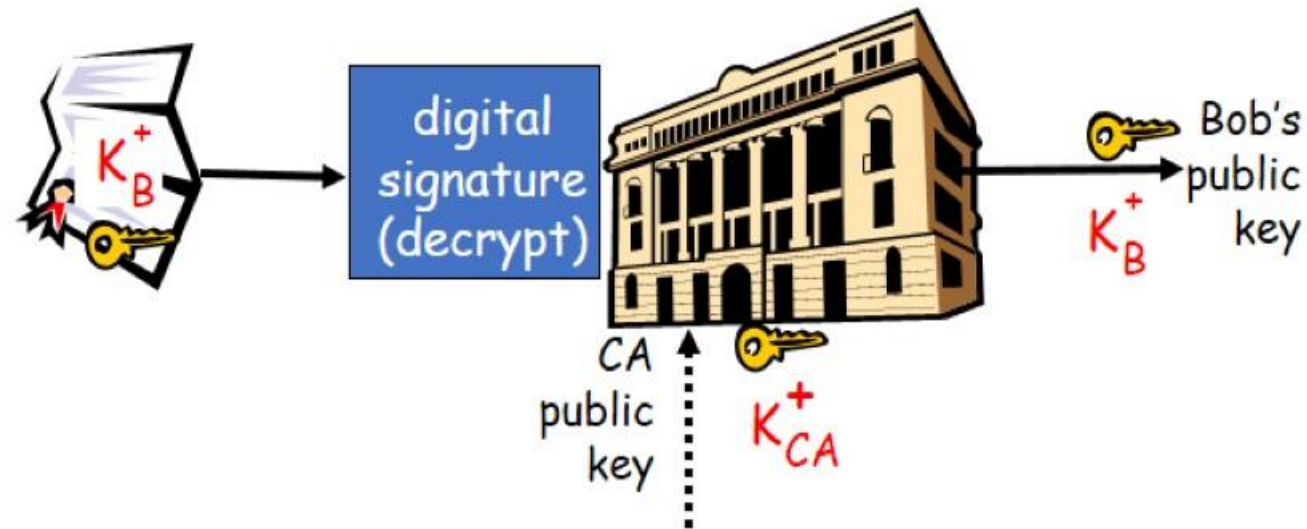


- **Certification authority (CA):** binds a public key to a particular entity, E.
- E (person, router) registers its public key with CA.
 - E provides “proof of identity” to CA.
 - CA creates certificate binding E to its public key.
 - Certificate containing E’s public key digitally signed by CA – CA says “this is E’s public key”





- When Alice wants Bob's public key:
 - gets Bob's certificate (Bob or elsewhere).
 - apply CA's public key to Bob's certificate, get Bob's public key





➤ Problems

- Single administration trusted by all principals
- Single point of failure
- Scalability

➤ Solutions: break into multiple domains

- Each domain has a trusted administration



➤ **Secret keys:**

- KDCs share pairwise key
- topology of KDC: tree with shortcuts

➤ **Public keys:**

- cross-certification of CAs
- example: Alice with CA_A , Boris with CA_B
 - Alice gets CA_B 's certificate (public key p_1), signed by CA_A
 - Alice gets Boris' certificate (its public key p_2), signed by CA_B (p_1)



This part explained :

- Biometrics Usage
- Phases of Biometric System
- Authentication in distributed systems
 - Smart Card
 - Microsoft Passport
- Key Distribution Center (KDC)
- Certification Authorities (CA)



Databases Security



- Database administrator – Set a rules for users
- Database management system (DBMS) – Through which user interaction with DB
- Record – Raws
- Field/element - Contents
- Schema - Structure of DB
- Subschema – For specific user
- Attribute - Columns
- Relation – a set of DB Columns



- `SELECT ZIP='43210'`

Name	First	Address	City	State	Zip	Airport
ADAMS	Charles	212 Market St.	Columbus	OH	43210	CMH
ADAMS	Edward	212 Market St.	Columbus	OH	43210	CMH
CARTER	Marlene	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Beth	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Ben	411 Elm St.	Columbus	OH	43210	CMH
CARTER	<u>Lisabeth</u>	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Mary	411 Elm St.	Columbus	OH	43210	CMH



- **Reliability:** in the context of databases, reliability is the ability to run for long periods without failing
- **Database integrity:** concern that the database as a whole is protected against damage
- **Element integrity:** concern that the value of a specific data element is written or changed only by authorized users
- **Element accuracy:** concern that only correct values are written into the elements of a database



- **Phase 1: Intent**
 - DBMS does everything it can, other than making changes to the database, to **prepare for the update**
 - Collects records, opens files, locks out users, makes calculations
 - DBMS commits by writing a commit flag to the database
- **Phase 2: Write**
 - DBMS completes all write operations
 - DBMS removes the commit flag
- If the DBMS fails during either phase 1 or phase 2, it can be restarted and repeat that phase without causing harm



- Error detection and correction codes to protect data integrity
- For recovery purposes, a database can maintain a change log, allowing it to repeat changes as necessary when recovering from failure
- Databases use locks and atomic operations to maintain consistency
 - Writes are treated as atomic operations
 - Records are locked during write so they cannot be read in a partially updated state



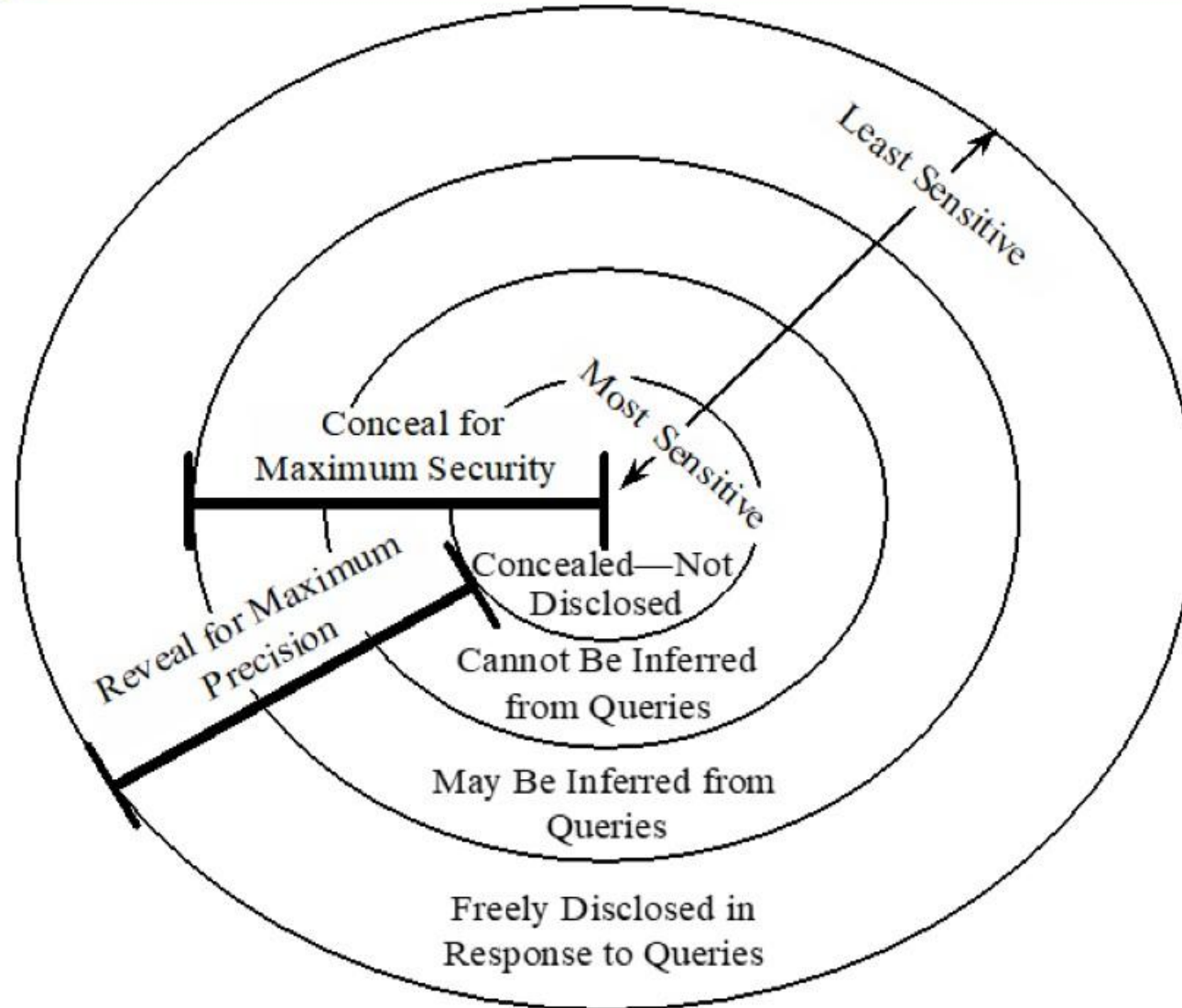
- Keeping records from being **dumped out** of the database is not sufficient to actually prevent disclosure.
- There are many ways to **deduce** the content of a database.
- Apply the appropriate **protection mechanisms** to protect sensitive database information.



- Suppress obviously sensitive information
- Keep track of what each user knows based on past queries
- Disguise the data



Security vs. Precision





- **Data mining** uses statistics, machine learning, mathematical models, pattern recognition, and other techniques to discover patterns and relations on large datasets
- The size and value of the datasets present an important security and privacy challenge, as the consequences of disclosure are naturally high



- Correcting mistakes in data
- Preserving privacy
- Secure data storage
- Transaction logs
- Real-time security monitoring



This part explained :

- Database security requirements include.
- Reliability and Integrity
- Two-Phase Update
- There are many subtle ways for sensitive data to be inadvertently disclosed, and there is no single answer for prevention
- Data mining and big data have numerous open security and privacy challenges



Thank You