IT344 – DATABASE MANAGEMENT
CHAPTER: 24
WEEK: 10
---

1 Introduction to Database Security Issues

- **Types of Security**
  - Legal and ethical issues
  - Policy issues
  - System-related issues
  - The need to identify multiple security levels

- أنواع الأمن
  - المسائل القانونية والأخلاقية
  - مشكلة سياسية
  - المسائل المتعلقة بالنظام
  - الحاجة إلى تحديد مستويات أمنية متعددة

- **Threats to databases**

1- Loss of integrity
2- Loss of availability
3- Loss of confidentiality

To protect databases against these types of threats four kinds of countermeasures can be implemented:

- Access control
- Inference control
- Flow control
- Encryption

- التهديدات لقواعد البيانات
  1- فقدان السلامة
  2- فقدان التوافر
  3- فقدان السرية

- ولحماية قواعد البيانات ضد هذه الأنواع من التهديدات يمكن تنفيذ أربعة أنواع من التدابير المضادة:
  1- صلاحية تحكم الدخول
  2- التحكم في الاستدلال
  3- التحكم في التدفق
  4- التشفير

- A DBMS typically includes a database security and authorization subsystem that is responsible for ensuring the security portions of a database against unauthorized access.

- Two types of database security mechanisms:

Discretionary security mechanisms
Mandatory security mechanisms

- يتضمن نظام إدارة قواعد البيانات عادة نظام أمان قاعدة بيانات والتخويل يكون مسؤولا عن ضمان الأجزاء الأمنية لقاعدة البيانات ضد الوصول غير المصرح به.

- نوعان من آليات أمن قاعدة البيانات:
- آليات أمنية تقديرية
- آليات أمنية إلزامية

- The security mechanism of a DBMS must include provisions for restricting access to the database as a whole

- This function is called access control and is handled by creating user accounts and passwords to control login process by the DBMS.

- ويجب أن تتضمن الآلية الأمنية لنظام إدارة قواعد البيانات أحكاما تقيد الوصول إلى قاعدة البيانات ككل

- وتسمى هذه الدالة التحكم بالوصول ويتم التعامل معها من خلال إنشاء حسابات المستخدمين وكلمات المرور للتحكم في عملية تسجيل الدخول بواسطة نظام إدارة قاعدة البيانات.

- The security problem associated with databases is that of controlling the access to **a statistical database**, which is used to provide statistical information or summaries of values based on various criteria.

- The countermeasures to **statistical database security** problem is called **inference control measures.**

- والمشكلة الأمنية المرتبطة بقواعد البيانات هي التحكم في الوصول إلى قاعدة بيانات إحصائية تستخدم لتوفير معلومات إحصائية أو ملخصات للقيم استنادا إلى معايير مختلفة.

- وتسمى التدابير المضادة لمشكلة أمن قاعدة البيانات الإحصائية تدابير مراقبة الاستدلال.

- Another security is that of **flow control**, which prevents information from flowing in such a way that it reaches unauthorized users.
- Channels that are pathways for information to flow implicitly in ways that violate the security policy of an organization are called **covert channels**.

- وثمة أمن آخر هو التحكم في التدفق، الذي يمنع تدفق المعلومات بطريقة تصل إلى المستخدمين غير المصرح لهم.
- القنوات التي هي مسارات لتدفق المعلومات ضمنيا بطرق تنتهك سياسة الأمن لمنظمة ما تسمى قنوات سرية.

- A final security issue is **data encryption**, which is used to protect sensitive data (such as credit card numbers) that is being transmitted via some type communication network.
- The data is **encoded** using some **encoding algorithm**.
  - An unauthorized user who access encoded data will have difficulty deciphering it, but authorized users are given decoding or decrypting algorithms (or keys) to decipher data.

- وهناك مشكلة أمنية نهائية هي تشفير البيانات، الذي يستخدم لحماية البيانات الحساسة (مثل أرقام بطاقات الائتمان) التي يتم إرسالها عبر بعض نوع شبكات الإتصال.
- يتم ترميز البيانات باستخدام بعض خوارزمية التشفير.
  - سيتعذر على المستخدم غير المصرح له أن يصل إلى البيانات المشفرة وفك رموزه، ولكن يتم منح المستخدمين المرخص لهم فك تشفير أو فك تشفير الخوارزميات (أو المفاتيح) لفك البيانات.

1.2 Database Security and the DBA

- The database administrator (**DBA**) is the central authority for managing a database system.
  - The DBA's responsibilities include
    - granting privileges to users who need to use the system
    - classifying users and data in accordance with the policy of the organization
- The DBA is responsible for the overall security of the database system.

- مسؤول قاعدة البيانات (DBA) هو السلطة المركزية لإدارة نظام قاعدة البيانات.
- وتشمل مسؤوليات DBA
  - منح امتيازات للمستخدمين الذين يحتاجون إلى استخدام النظام
  - وتصنيف المستخدمين والبيانات وفقا لسياسة المنظمة
  - و DBA هو المسؤول عن الأمن الشامل لنظام قاعدة البيانات.

- The DBA has a DBA account in the DBMS
  - Sometimes these are called a system or superuser account
  - These accounts provide powerful capabilities such as:
    - 1. Account creation
    - 2. Privilege granting
    - 3. Privilege revocation
    - 4. Security level assignment
  - Action 1 is access control, whereas 2 and 3 are discretionary and 4 is used to control mandatory authorization

- يحتوي DBA على حساب DBA في DBMS
  - في بعض الأحيان هذه تسمى نظام أو حساب المستخدم المتميز
  - توفر هذه الحسابات قدرات قوية مثل:
    - 1- إنشاء حساب
    - 2- منح الامتيازات
    - 3- إلغاء الامتيازات
    - 4- تخصيص مستوى الأمان
- الإجراء 1 هو التحكم في الوصول (النفاذ)، 2 و 3 هما تقديران و 4 يستخدم للتحكم في الإذن الإلزامي

1.3 **Access Protection, User Accounts, and Database Audits**

- Whenever a person or group of person s need to access a database system, the individual or group must first apply for a user account.
  - The DBA will then create a new **account id** and **password** for the user if he/she deems there is a legitimate need to access the database
- The user must log in to the DBMS by entering account id and password whenever database access is needed.

- كلما كان الشخص أو مجموعة من الأشخاص بحاجة إلى الوصول إلى نظام قاعدة البيانات، يجب على الفرد أو المجموعة أولا طلب الحصول على حساب المستخدم.
- سيقوم DBA إنشاء معرف حساب جديد وكلمة مرور للمستخدم إذا كان هو / هي ترى أن هناك حاجة مشروعة للوصول إلى قاعدة البيانات
- يجب على المستخدم تسجيل الدخول إلى DBMS عن طريق إدخال معرف الحساب وكلمة المرور كلما كان هناك حاجة إلى الوصول إلى قاعدة البيانات.

- The database system must also keep **track of all operations** on the database that are applied by a certain user throughout **each login session**.
  - To keep a record of all updates applied to the database and of the particular user who applied each update, we can modify **system log**, which includes an entry for each operation applied to the database that may be required for recovery from a transaction failure or system crash.

- يجب أيضا على نظام قاعدة البيانات تتبع جميع العمليات على قاعدة البيانات التي يتم تطبيقها من قبل مستخدم معين طوال كل جلسة تسجيل الدخول.
- للاحتفاظ بسجل لكافة التحديثات المطبقة على قاعدة البيانات والمستخدم المحدد الذي قام بتطبيق كل تحديث، يمكننا تعديل سجل النظام الذي يتضمن إدخال لكل عملية يتم تطبيقها على قاعدة البيانات التي قد تكون مطلوبة للاسترداد من فشل أو تصادم في نظام المعاملة.

- If any tampering with the database is suspected, a **database audit** is performed
  - A database audit consists of reviewing the log to examine all accesses and operations applied to the database during a certain time period.
- A database log that is used mainly for security purposes is sometimes called an **audit trail**.

- إذا تم التلاعب بأي قاعدة بيانات، يتم إجراء تدقيق قاعدة البيانات
- وتتكون مراجعة قاعدة البيانات من استعراض السجل لفحص جميع عمليات الدخول والعمليات المطبقة على قاعدة البيانات خلال فترة زمنية معينة.
- ويسمى أحيانا سجل قاعدة البيانات الذي يستخدم أساسا لأغراض أمنية مسارا للتدقيق.

The typical method of enforcing discretionary access control in a database system is based on the granting and revoking privileges.

- وتستند الطريقة النمطية لفرض التحكم في النفاذ إلى المعلومات التقديري في نظام قاعدة البيانات إلى منح الامتيازات وإبطالها.

2.1Types of Discretionary Privileges

- The **account level**:
  - At this level, the DBA specifies the particular privileges that each account holds independently of the relations in the database.
- The **relation level** (or **table level**):
  - At this level, the DBA can control the privilege to access each individual relation or view in the database.

- مستوى الحساب:
  - في هذا المستوى، يحدد DBA الامتيازات الخاصة التي يحملها كل حساب بشكل مستقل عن العلاقات في قاعدة البيانات.
- مستوى العلاقة (أو مستوى الجدول):
  - في هذا المستوى، يمكن DBA السيطرة على امتياز للوصول إلى كل علاقة فردية أو عرض في قاعدة البيانات.

- The privileges at the **account level** apply to the capabilities provided to the account itself and can include
  - the **CREATE SCHEMA** or **CREATE TABLE** privilege, to create a schema or base relation;
  - the **CREATE VIEW** privilege;
  - the **ALTER** privilege, to apply schema changes such adding or removing attributes from relations;
  - the **DROP** privilege, to delete relations or views;
  - the **MODIFY** privilege, to insert, delete, or update tuples;
  - and the **SELECT** privilege, to retrieve information from the database by using a **SELECT** query.

- تنطبق الامتيازات على مستوى الحساب على القدرات المقدمة للحساب نفسه ويمكن أن تشمل:
  - CREATE SCHEMA أو CREATE TABLE لإنشاء مخطط أو قاعدة العلاقة.
  - امتياز CREATE VIEW
  - امتياز ALTER ، لتطبيق مخطط يتغير مثل إضافة أو إزالة سمات العلاقات.
  - امتياز DROP ، لحذف العلاقات أو العرض.
  - امتياز MODIFY ، لإدراج أو حذف أو تعديل الصفوف.
  - امتياز SELECT ، لإسترداد المعلومات من قاعدة البيانات باستخدام استعلام SELECT.

- The second level of privileges applies to the **relation level**
  - This includes **base relations** and virtual (**view**) relations.
- The granting and revoking of privileges generally follow an authorization model for discretionary privileges known as the access matrix model where
  - The **rows** of a matrix M represents **subjects** (users, accounts, programs)
  - The **columns** represent **objects** (relations, records, columns, views, operations).
  - Each position **M(i,j)** in the matrix represents the types of privileges (read, write, update) that **subject i** holds on **object j**.

- وينطبق المستوى الثاني من الامتيازات على مستوى العلاقة
  - وهذا يشمل العلاقات الأساسية والعلاقات الافتراضية (عرض).
- ويتبع منح الامتيازات وإلغائها عموما نموذج ترخيص للامتيازات التقديرية المعروفة باسم نموذج مصفوفة النفاذ حيثما يكون
- الصفوف من مصفوفة M تمثل المواضيع (المستخدمين والحسابات والبرامج)
- تمثل الأعمدة العناصر (العلاقات، السجلات، الأعمدة، المشاهدات، العمليات).
- ويمثل كل موقف M (i,j) في المصفوفة أنواع الامتيازات (قراءة، كتابة، تحديث) الموضوع الذي يحمله على الكائن j.

- To control the granting and revoking of relation privileges, each relation R in a database is assigned and **owner account**, which is typically the account that was used when the relation was created in the first place.
  - The owner of a relation is given all privileges on that relation.
  - In SQL2, the DBA can assign and owner to a whole schema by creating the schema and associating the appropriate authorization identifier with that schema, using the **CREATE SCHEMA** command.
  - The owner account holder can **pass privileges** on any of the owned relation to other users by **granting** privileges to their accounts.

- للتحكم في منح وإلغاء امتيازات العلاقة، يتم تعيين كل علاقة R في قاعدة بيانات وحساب المالك، وهو عادة الحساب الذي تم استخدامه عند إنشاء العلاقة في المقام الأول.
- يمنح صاحب العلاقة جميع الامتيازات في تلك العلاقة.
- في SQL2، يمكن تخصيص DBA والمالك إلى مخطط كامل من خلال إنشاء المخطط وربط معرف المصادقة المناسب مع هذا المخطط باستخدام الأمر CREATE SCHEMA
- يمكن لمالك حساب المالك اجتياز الامتيازات على أي من العلاقة المملوكة للمستخدمين الآخرين من خلال منح امتيازات لحساباتهم.

- In SQL the following types of privileges can be granted on each individual relation R:
  - **SELECT** (retrieval or read) privilege on R:
    - Gives the account retrieval privilege.
    - In SQL this gives the account the privilege to use the **SELECT** statement to retrieve tuples from R.
  - **MODIFY** privileges on R:
    - This gives the account the capability to modify tuples of R.
    - In SQL this privilege is further divided into **UPDATE**, **DELETE**, and **INSERT** privileges to apply the corresponding SQL command to R.
    - In addition, both the **INSERT** and **UPDATE** privileges can specify that only certain attributes can be updated by the account.

- في SQL يمكن منح الأنواع التالية من الامتيازات على كل علاقة فردية R:
- SELECT (استرجاع أو قراءة) امتياز على R:
- يعطي امتياز استرجاع الحساب.
- في SQL هذا يعطي الحساب امتياز لاستخدام عبارة SELECT لاسترداد صفوف من R.
- امتيازات التعديل على R:
- وهذا يعطي الحساب القدرة على تعديل الصفوف من R.
- في SQL يتم تقسيم هذا الامتياز أيضا إلى امتيازات INSERT, DELETE, UPDATE لتطبيق الأمر SQL المقابل إلى R.
- بالإضافة إلى ذلك، يمكن لكل من امتيازات INSERT and UPDATE تحديد أنه يمكن تحديث سمات معينة فقط بواسطة الحساب.

- In SQL the following types of privileges can be granted on each individual relation R (contd.):
  - **REFERENCES** privilege on R:
    - This gives the account the capability to **reference** relation R when specifying integrity constraints.
    - The privilege can also be **restricted** to specific attributes of R.
- Notice that to create a **view**, the account must have **SELECT** privilege on all relations involved in the view definition.

- في SQL يمكن منح الأنواع التالية من الامتيازات على كل علاقة فردية R :
- REFERENCES الامتياز على R:
- وهذا يعطي الحساب القدرة على الرجوع إلى العلاقة R عند تحديد قيود النزاهة.
- ويمكن أيضا أن يقتصر الامتياز على سمات محددة من R.
- لاحظ أنه لإنشاء ملف شخصي، يجب أن يكون للحساب امتياز SELECT على جميع العلاقات التي ينطوي عليها تعريف الملف الشخصي.

2.2 Specifying Privileges Using Views

- The mechanism of **views** is an important discretionary authorization mechanism in its own right. For example,
  - If the owner A of a relation R wants another account B to be able to retrieve only some fields of R, then A can create a view V of R that includes only those attributes and then grant SELECT on V to B.
  - The same applies to limiting B to retrieving only certain tuples of R; a view V' can be created by defining the view by means of a query that selects only those tuples from R that A wants to allow B to access.

- وآلية العرض هي آلية تفويض تقديرية هامة في حد ذاتها. فمثلا،
- إذا كان المالك A من العلاقة R يريد حساب آخر B لتكون قادرة على استرداد فقط بعض حقول R ثم يمكن إنشاء عرض V من R الذي يتضمن فقط تلك السمات ومن ثم منح SELECT على V إلى B.
- وينطبق الشيء نفسه على الحد B لاسترجاع فقط بعض صفوف من R؛ يمكن إنشاء عرض V 'من خلال تحديد طريقة العرض من خلال استعلام يحدد فقط تلك المعالجات من R التي تريد A السماح B للوصول إليها.

2.3 Revoking Privileges

- In some cases it is desirable to grant a privilege to a user temporarily. For example,
  - The owner of a relation may want to grant the **SELECT** privilege to a user for a specific task and then revoke that privilege once the task is completed.
  - Hence, a mechanism for **revoking** privileges is needed. In SQL, a **REVOKE** command is included for the purpose of **canceling privileges**.

- في بعض الحالات، من المستحسن منح امتياز للمستخدم مؤقتا. فمثلا،
- قد يرغب مالك العلاقة في منح امتياز SELECT لمستخدم معين لمهمة معينة ثم إلغاء هذا الامتياز بعد اكتمال المهمة.
- وبالتالي، هناك حاجة إلى آلية لإلغاء الامتيازات. في SQL، يتم تضمين الأمر REVOKE لغرض إلغاء الامتيازات.

2.4 Propagation of Privileges using the GRANT OPTION

- Whenever the owner A of a relation R grants a privilege on R to another account B, privilege can be given to B with or without the **GRANT OPTION**.
- If the **GRANT OPTION** is given, this means that B can also grant that privilege on R to other accounts.
  - Suppose that B is given the **GRANT OPTION** by A and that B then grants the privilege on R to a third account C, also with **GRANT OPTION**. In this way, privileges on R can **propagate** to other accounts without the knowledge of the owner of R.
  - If the owner account A now revokes the privilege granted to B, all the privileges that B propagated based on that privilege should automatically be revoked by the system.

- عندما يمنح المالك A من العلاقة R امتيازا على R لحساب آخر B، يمكن منح الامتياز ل B مع أو بدون "GRANT OPTION".
- إذا أعطيت GRANT OPTION ، وهذا يعني أن B يمكن أيضا منح هذا الامتياز على R إلى حسابات أخرى.
- لنفترض أن B تعطى "GRANT OPTION " من A، ثم B منح الامتياز على R لحساب ثالث C، أيضا مع GRANT OPTION. وبهذه الطريقة، يمكن للامتيازات على R أن تنتشر إلى حسابات أخرى دون علم صاحب R.
- إذا ألغى حساب المالك (A) الآن الامتياز الممنوح ل B، فإن جميع الامتيازات التي تم نشرها B بناء على هذا الامتياز يجب أن يتم إبطالها تلقائيا من قبل النظام.

2.5 An Example

- Suppose that the DBA creates four accounts
  - A1, A2, A3, A4
- and wants only A1 to be able to create base relations. Then the DBA must issue the following GRANT command in SQL

GRANT CREATETAB TO A1;

- In SQL2 the same effect can be accomplished by having the DBA issue a **CREATE SCHEMA** command as follows:
  CREATE SCHAMA EXAMPLE **AUTHORIZATION** A1;

- لنفترض أن DBA ينشئ أربعة حسابات
- A1، A2، A3، A4
- ويريد فقط A1 لتكون قادرة على إنشاء العلاقات الأساسية. ثم DBA يجب إصدار الأمر GRANT التالية في SQL
- منحة CREATETAB إلى A1؛
- في SQL2 يمكن تحقيق نفس التأثير من خلال وجود DBA CREATE SCHEMA كما يلي:
- CREATE SCHAMA EXAMPLE AUTHORIZATION A1

1-

2.5 An Example (2)

- User account A1 can create tables under the schema called **EXAMPLE**.
- Suppose that A1 **creates** the two base relations **EMPLOYEE** and **DEPARTMENT**
  - A1 is then **owner** of these two relations and hence all the relation privileges on each of them.
- Suppose that A1 wants to grant A2 the privilege to insert and delete tuples in both of these relations, but A1 does not want A2 to be able to propagate these privileges to additional accounts:
  GRANT INSERT, DELETE ON
  EMPLOYEE, DEPARTMENT **TO A2;**

- يمكن لحساب المستخدم A1 إنشاء جداول ضمن المخطط المسمى EXAMPLE.
- افترض أن A1 ينشئ اثنين من العلاقات الأساسية الموظف والإدارة
- A1 صاحب هذه العلاقات، وبالتالي كل امتيازات العلاقة على كل واحد منهم.
- لنفترض أن A1 يريد منح A2 امتياز إدراج وحذف صفوف في كل من هذه العلاقات، ولكن A1 لا يريد A2 أن يكون قادرا على نشر هذه الامتيازات إلى حسابات إضافية:
- GRANT INSERT, DELETE ON
- EMPLOYEE, DEPARTMENT **TO A2;**

2.5 An Example (3)

EMPLOYEE

Name	Ssn	Bdate	Address	Sex	Salary	Dno

DEPARTMENT

Dnumber	Dname	Mgr_ssn

Figure 24.1
Schemas for the two relations EMPLOYEE and DEPARTMENT.

2.5 An Example (4)

- Suppose that A1 wants to allow A3 to retrieve information from either of the two tables and also to be able to propagate the SELECT privilege to other accounts.
- A1 can issue the command:
  GRANT SELECT ON EMPLOYEE, DEPARTMENT
  TO A3 **WITH GRANT OPTION;**
- A3 can grant the **SELECT** privilege on the **EMPLOYEE** relation to A4 by issuing:
  GRANT SELECT ON EMPLOYEE **TO** A4;
  - Notice that A4 can't propagate the SELECT privilege because GRANT OPTION was not given to A4

- افترض أن A1 يريد السماح A3 باسترداد المعلومات من أي من الجدولين وأيضا لتكون قادرة على نشر امتياز SELECT إلى حسابات أخرى.
- A1 يمكن إصدار الأمر:
- GRANT SELECT ON EMPLOYEE, DEPARTMENT
- TO A3 WITH GRANT OPTION;
- A3 يمكن منح امتياز SELECT على علاقة الموظف ب A4 من خلال إصدار:
- GRANT SELECT ON EMPLOYEE TO A4;
- لاحظ أن A4 لا يمكن نشر امتياز SELECT لأنه لم يتم منح GRANT OPTION إلى A4

2.5 An Example (5)

- Suppose that A1 decides to revoke the SELECT privilege on the EMPLOYEE relation from A3; A1 can issue:
  REVOKE SELECT ON EMPLOYEE **FROM** A3**;**
- The DBMS must now automatically revoke the SELECT privilege on EMPLOYEE from A4, too, because A3 granted that privilege to A4 and A3 does not have the privilege any more.

- لنفترض أن A1 يقرر إلغاء امتياز SELECT على علاقة الموظف من A3؛ A1 يمكن أن يصدر:
- REVOKE SELECT ON EMPLOYEE FROM A3;
- يجب على DBMS الآن إلغاء امتياز SELECT على الموظف تلقائيا من A4، أيضا، لأن A3 لم تمنح هذا الامتياز ل A4 و A3 ليس لديه امتيازات أكثر من ذلك.

2.5 An Example (6)

- Suppose that A1 wants to give back to A3 a limited capability to SELECT from the EMPLOYEE relation and wants to allow A3 to be able to propagate the privilege.
- The limitation is to retrieve only the NAME, BDATE, and ADDRESS attributes and only for the tuples with DNO=5.
- A1 then create the view:
- **CREATE VIEW** A3EMPLOYEE **AS**
- **SELECT** NAME, BDATE, ADDRESS
- **FROM** EMPLOYEE
- **WHERE** DNO = 5**;**
- After the view is created, A1 can grant **SELECT** on the view A3EMPLOYEE to A3 as follows:
- **GRANT SELECT ON** A3EMPLOYEE **TO** A3
- **WITH GRANT OPTION;**

- لنفترض أن A1 يريد أن يعيد إلى A3 قدرة محدودة على SELECT من علاقة الموظف ويريد أن يسمح A3 لتكون قادرة على نشر الامتياز.
- ويتمثل الحد في استرداد سمات NAME و BDATE و ADDRESS فقط للصفوف مع DNO = 5.
- A1 ثم إنشاء عرض:

```
CREATE VIEW A3EMPLOYEE AS
SELECT NAME, BDATE, ADDRESS
FROM EMPLOYEE
WHERE DNO = 5;
```

- بعد إنشاء طريقة العرض، يمكن A1 منح SELECT على عرض A3EMPLOYEE إلى A3 كما يلي:

```
GRANT SELECT ON A3EMPLOYEE TO A3
WITH GRANT OPTION;
```

2.5 An Example (7)

- Finally, suppose that A1 wants to allow A4 to update only the SALARY attribute of EMPLOYEE;
- A1 can issue:
- **GRANT UPDATE ON** EMPLOYEE **(**SALARY**) TO** A4**;**
- The **UPDATE** or **INSERT** privilege can specify particular attributes that may be updated or inserted in a relation.
- Other privileges (**SELECT**, **DELETE**) are not attribute specific.

- وأخيرا، افترض أن A1 يريد السماح ل A4 بتحديث سمة SALARY للموظف فقط؛
- A1 يمكن أن يصدر:

```
GRANT UPDATE ON EMPLOYEE (SALARY) TO A4;
```

- يمكن أن يحدد امتياز UPDATE or INSERT سمات معينة قد يتم تحديثها أو إدراجها في علاقة.
- امتيازات أخرى (SELECT, DELETE)ليست سمة محددة.

2.6 **Specifying Limits on Propagation of Privileges**

- Techniques to limit the propagation of privileges have been developed, although they have not yet been implemented in most DBMSs and are not a part of SQL.
  - Limiting **horizontal propagation** to an integer number i means that an account B given the GRANT OPTION can grant the privilege to at most i other accounts.
  - **Vertical propagation** is more complicated; it limits the depth of the granting of privileges.

- وقد وضعت تقنيات للحد من انتشار الامتيازات، على الرغم من أنها لم تنفذ بعد في معظم أنظمة إدارة قواعد البيانات ولا تشكل جزءا من SQL.
- ويقصد بالحد من الانتشار الأفقي لرقم صحيح i أن الحساب B الذي يمنح " GRANT OPTION " يمكن أن يمنح الامتياز في معظم الحالات لحسابات أخرى.
- ويكون الانتشار العمودي أكثر تعقيدا؛ فإنه يحد من عمق منح الامتيازات.

3 Mandatory Access Control and Role-Based Access Control for Multilevel Security

- The discretionary access control techniques of granting and revoking privileges on relations has traditionally been the main security mechanism for relational database systems.
- This is an all-or-nothing method:
  - A user either has or does not have a certain privilege.
- In many applications, and **additional security policy** is needed that classifies data and users based on security classes.
  - This approach as **mandatory access control**, would typically be **combined** with the discretionary access control mechanisms.

- وقد كانت الأساليب التقديرية لمراقبة الدخول في منح الامتيازات وإلغاءها على العلاقات هي الآلية الأمنية الرئيسية لنظم قواعد البيانات العلائقية.
- هذا هو كل شيء أو لا شيء:
- يمتلك المستخدم امتيازا معينا أو لا يمتلكه.
- في العديد من التطبيقات، وهناك حاجة إلى سياسة أمنية إضافية التي تصنف البيانات والمستخدمين على أساس فئات الأمن.
- ومن شأن هذا النهج باعتباره التحكم الإلزامي في النفاذ، أن يقترن عادة بآليات مراقبة الدخول التقديرية.

- Typical **security classes** are top secret (TS), secret (S), confidential (C), and unclassified (U), where TS is the highest level and U the lowest: TS ≥ S ≥ C ≥ U
- The commonly used model for multilevel security, known as the Bell-LaPadula model, classifies each **subject** (user, account, program) and **object** (relation, tuple, column, view, operation) into one of the security classifications, T, S, C, or U:
  - **Clearance** (classification) of a subject S as **class(S)** and to the **classification** of an object O as **class(O)**.

- وتكون فئات الأمن النموذجية سرية للغاية (TS) والسرية (S) والسرية (C) وغير المصنفة (U)، حيث TS هي أعلى مستوى و U أدنى: تيسي S ≥ C ≥ U ≤
-
- النموذج الذي يشيع استخدامه للأمن متعدد المستويات، والمعروف باسم نموذج Bell-LaPadula، يصنف كل موضوع (المستخدم والحساب والبرنامج) والهدف (العلاقة، التوأم، العمود، العرض، العملية) في أحد تصنيفات الأمن، T، S، C أو U:
- التخليص (التصنيف) لموضوع S كفئة (S) وتصنيف كائن O كفئة (O).

- Two restrictions are enforced on data access based on the subject/object classifications:
  - **Simple security property:** A subject S is not allowed read access to an object O unless class(S) ≥ class(O).
  - A subject S is not allowed to write an object O unless class(S) ≤ class(O). This known as the **star property** (or * property).

- ويتم فرض قيود على الوصول إلى البيانات استنادا إلى تصنيف الموضوع / الكائن:
- خاصية الأمان البسيطة: لا يسمح للموضوع S بالدخول للقراءة إلى كائن O ما لم تكن الفئة (S) ≤ الفئة (O).
- لا يسمح للموضوع S بكتابة كائن O ما لم تكن الفئة (S) ≥ فئة (O). وهذا يعرف باسم خاصية النجمة (أو * الخاصية).

- To incorporate multilevel security notions into the relational database model, it is common to consider attribute values and tuples as data objects.
- Hence, each attribute A is associated with a **classification attribute C** in the schema, and each attribute value in a tuple is associated with a corresponding security classification.
- In addition, in some models, a **tuple classification** attribute TC is added to the relation attributes to provide a classification for each tuple as a whole.
- Hence, a **multilevel relation** schema R with n attributes would be represented as
  - $R(A_1,C_1,A_2,C_2, \ldots, A_n,C_n,TC)$
- where each Ci represents the classification attribute associated with attribute A_i.

- لدمج المفاهيم الأمنية متعددة المستويات في نموذج قاعدة البيانات العلائقية، من الشائع النظر في قيم السمات والصفوف ككائنات بيانات.
- وبالتالي، يتم ربط كل سمة A مع سمة تصنيف C في المخطط، وكل قيمة سمة في صفوف مقترنة بتصنيف أمان مطابق.
- وبالإضافة إلى ذلك، في بعض النماذج، يتم إضافة سمة تصنيف صفوف إلى سمات العلاقة لتوفير تصنيف لكل صف ككل.
- وبالتالي، فإن مخطط R متعدد المستويات R مع سمات n سيتم تمثيل كما
- R (A1، C1، A2، C2، ...، A_n,C_n,TC)
- حيث تمثل كل Ci السمة التصنيف المرتبطة بالسمة A_i.

- The value of the **TC** attribute in each tuple t – which is the highest of all attribute classification values within t – provides a general classification for the tuple itself, whereas each C_i provides a finer security classification for each attribute value within the tuple.
  - The apparent key of a multilevel relation is the set of attributes that would have formed the primary key in a regular (single-level) relation.

- توفر قيمة السمة TC في كل صفوف t - وهو أعلى قيم تصنيف السمات داخل t - تصنيفا عاما للصفوف نفسها، في حين توفر كل C تصنيفا أمنيا أكثر دقة لكل قيمة سمة داخل الصفوف.
- المفتاح الظاهر لعلاقة متعددة المستويات هو مجموعة السمات التي كانت ستشكل المفتاح الأساسي في علاقة منتظمة (على مستوى واحد).

- A multilevel relation will appear to contain different data to subjects (users) with different clearance levels.
  - In some cases, it is possible to store a single tuple in the relation at a higher classification level and produce the corresponding tuples at a lower-level classification through a process known as **filtering**.
  - In other cases, it is necessary to store two or more tuples at different classification levels with the same value for the **apparent key**.
- This leads to the concept of **polyinstantiation** where several tuples can have the same apparent key value but have different attribute values for users at different classification levels.

- يبدو أن العلاقة متعددة المستويات تحتوي على بيانات مختلفة للمواضيع (المستخدمين) مع مستويات التخليص المختلفة.
- في بعض الحالات، فمن الممكن لتخزين صف واحد في العلاقة على مستوى تصنيف أعلى وإنتاج الموازين المقابلة في تصنيف المستوى الأدنى من خلال عملية تعرف باسم التصفية.
- في حالات أخرى، فمن الضروري لتخزين اثنين أو أكثر من الصفوف في مستويات تصنيف مختلفة مع نفس القيمة للمفتاح الظاهري.
- وهذا يؤدي إلى مفهوم polyinstantiation حيث العديد من الصفوف يمكن أن يكون لها نفس القيمة الرئيسية واضحة ولكن لديها قيم السمة مختلفة للمستخدمين في مستويات التصنيف المختلفة.

- In general, the **entity integrity** rule for multilevel relations states that all attributes that are members of the apparent key must not be null and must have the same security classification within each individual tuple.
- In addition, all other attribute values in the tuple must have a security classification greater than or equal to that of the apparent key.
  - This **constraint** ensures that a user can see the key if the user is permitted to see any part of the tuple at all.

- وبوجه عام، فإن قاعدة سلامة الكيان للعلاقات متعددة المستويات تنص على أن جميع الصفات التي هي أعضاء في المفتاح الظاهر يجب ألا تكون خالية ويجب أن يكون لها نفس التصنيف الأمني داخل كل طبقة فردية.
- بالإضافة إلى ذلك، يجب أن يكون لكل قيم السمات الأخرى في صف تصنيف أمان أكبر من أو يساوي ذلك المفتاح الظاهري.
- ويضمن هذا القيد إمكانية رؤية المستخدم للمفتاح إذا سمح للمستخدم بالاطلاع على أي جزء من الصفوف.

- Other integrity rules, called **null integrity** and **interinstance integrity**, informally ensure that if a tuple value at some security level can be filtered (derived) from a higher-classified tuple, then it is sufficient to store the higher-classified tuple in the multilevel relation.

- قواعد السلامة الأخرى، وتسمى null integrity and interinstance integrity ، وضمان غير رسمي أنه إذا كان يمكن تصفية قيمة صفوف في بعض مستوى الأمن (مشتقة) من أعلى تصنيفا، ثم يكفي لتخزين أعلى تصنيفا في العلاقة متعددة المستويات .

3.1 Comparing Discretionary Access Control and Mandatory Access Control

- **Discretionary Access Control (DAC)** policies are characterized by a high degree of flexibility, which makes them suitable for a large variety of application domains.
  - The main drawback of **DAC** models is their vulnerability to malicious attacks, such as Trojan horses embedded in application programs.

- التحكم المطلق في الوصول (DAC) وتتميز السياسات بدرجة عالية من المرونة، مما يجعلها مناسبة لمجموعة كبيرة ومتنوعة من مجالات التطبيق.
- العيب الرئيسي لنماذج DAC هو ضعفها للهجمات الخبيثة، مثل أحصنة طروادة جزءا لا يتجزأ من برامج التطبيق.

- By contrast, mandatory policies ensure a high degree of protection in a way, they prevent any illegal flow of information.
- Mandatory policies have the drawback of being too rigid and they are only applicable in limited environments.
- In many practical situations, discretionary policies are preferred because they offer a better trade-off between security and applicability.

- وعلى النقيض من ذلك، فإن السياسات الإلزامية تضمن درجة عالية من الحماية بطريقة تمنع أي تدفق غير قانوني للمعلومات.
- السياسات الإلزامية لها عيب أن تكون جامدة جدا وأنها تنطبق فقط في بيئات محدودة.
- وفي كثير من الحالات العملية، تفضل السياسات التقديرية لأنها توفر مقايضة أفضل بين الأمن وقابلية التطبيق.

3.2 Role-Based Access Control

- **Role-based access control** (RBAC) emerged rapidly in the 1990s as a proven technology for managing and enforcing security in large-scale enterprisewide systems.
- Its basic notion is that permissions are associated with roles, and users are assigned to appropriate roles.
- Roles can be created using the CREATE ROLE and DESTROY ROLE commands.
  - The GRANT and REVOKE commands discussed under DAC can then be used to assign and revoke privileges from roles.

- التحكم في الوصول القائم على الدور (RBAC)
- ظهرت بسرعة في التسعينات باعتبارها تقنية ثابتة لإدارة وإنفاذ الأمن في نظم المشاريع الكبيرة.
- مفهومها الأساسي هو أن الأذونات ترتبط بالأدوار، ويتم تعيين المستخدمين إلى الأدوار المناسبة.
- يمكن إنشاء الأدوار باستخدام أوامر CREATE ROLE and DESTROY ROLE.
- ومن ثم يمكن استخدام أوامر GRANT and REVOKE التي نوقشت في إطار DAC لتعيين وإلغاء الامتيازات من الأدوار.

- RBAC appears to be a viable alternative to traditional discretionary and mandatory access controls; it ensures that only authorized users are given access to certain data or resources.
- Many DBMSs have allowed the concept of roles, where privileges can be assigned to roles.
- Role hierarchy in RBAC is a natural way of organizing roles to reflect the organization's lines of authority and responsibility.

- RBAC يبدو بديلا قابلا للتطبيق على الضوابط التقليدية التقديرية والإلزامية للنفاذ؛ فإنه يضمن أن يتم منح المستخدمين المصرح لهم فقط الوصول إلى بعض البيانات أو الموارد.
- وقد سمحت العديد من نظم إدارة قواعد البيانات بمفهوم الأدوار، حيث يمكن تعيين الامتيازات للأدوار.
- التسلسل الهرمي للأدوار في RBAC هو وسيلة طبيعية لتنظيم الأدوار لتعكس خطوط المنظمة من السلطة والمسؤولية.

- Another important consideration in RBAC systems is the possible temporal constraints that may exist on roles, such as time and duration of role activations, and timed triggering of a role by an activation of another role.
- Using an RBAC model is highly desirable goal for addressing the key security requirements of Web-based applications.
- In contrast, discretionary access control (DAC) and mandatory access control (MAC) models lack capabilities needed to support the security requirements emerging enterprises and Web-based applications.

- ومن الاعتبارات الهامة الأخرى في RBAC القيود الزمنية المحتملة التي يمكن أن تكون قائمة على الأدوار، مثل وقت ومدة تفعيل الأدوار، وتوقيت بدء دور من خلال تفعيل دور آخر.
- ويعد استخدام نموذج RBAC هدفا مرغوبا فيه للغاية لتلبية المتطلبات الأمنية الرئيسية للتطبيقات القائمة على الويب.
- وعلى النقيض من ذلك، تفتقر نماذج التحكم في النفاذ (DAC) والنماذج الإلزامية لمراقبة النفاذ (MAC) إلى القدرات اللازمة لدعم المتطلبات الأمنية للمؤسسات الناشئة والتطبيقات المستندة إلى الويب.

3.3 Access Control Policies for E-Commerce and the Web

- E-Commerce environments require elaborate policies that go beyond traditional DBMSs.
  - In an e-commerce environment the resources to be protected are not only traditional data but also knowledge and experience.
  - The access control mechanism should be flexible enough to support a wide spectrum of heterogeneous protection objects.
- A related requirement is the support for content-based access-control.

- تتطلب بيئات التجارة الإلكترونية سياسات تفصيلية تتجاوز نظم إدارة قواعد البيانات التقليدية.
- وفي بيئة التجارة الإلكترونية، فإن الموارد التي يتعين حمايتها ليست فقط بيانات تقليدية بل هي أيضا معرفة وخبرة.
- وينبغي أن تكون آلية التحكم في النفاذ مرنة بما فيه الكفاية لدعم طائفة واسعة من الأجسام غير المتجانسة للحماية.
- ويتمثل أحد المتطلبات ذات الصلة في دعم التحكم في النفاذ إلى المحتوى.

- Another requirement is related to the heterogeneity of subjects, which requires access control policies based on user characteristics and qualifications.
  - A possible solution, to better take into account user profiles in the formulation of access control policies, is to support the notion of credentials.
  - A credential is a set of properties concerning a user that are relevant for security purposes
    - For example, age, position within an organization
  - It is believed that the XML language can play a key role in access control for e-commerce applications.

- وثمة متطلب آخر يتعلق بعدم تجانس المواضيع، وهو ما يتطلب سياسات لمراقبة الدخول استنادا إلى خصائص المستعمل ومؤهلاته.
- ومن الحلول الممكنة، من أجل تحسين مراعاة ملفات المستخدمين في صياغة سياسات مراقبة الدخول، دعم فكرة وثائق التفويض.
- الاعتماد هو مجموعة من الخصائص المتعلقة بالمستخدم ذات الصلة لأغراض أمنية
- على سبيل المثال، العمر، والمنصب داخل المنظمة
- ويعتقد أن لغة شمل يمكن أن تلعب دورا رئيسيا في التحكم في الوصول لتطبيقات التجارة الإلكترونية.

4 Introduction to Statistical Database Security

- Another requirement is related to the heterogeneity of subjects, which requires access control policies based on user characteristics and qualifications.
  - A possible solution, to better take into account user profiles in the formulation of access control policies, is to support the notion of credentials.
  - A credential is a set of properties concerning a user that are relevant for security purposes
    - For example, age, position within an organization
  - It is believed that the XML language can play a key role in access control for e-commerce applications.

- وتستخدم قواعد البيانات الإحصائية أساسا لإنتاج إحصاءات عن مختلف السكان.
- قد تحتوي قاعدة البيانات على بيانات سرية عن الأفراد، والتي ينبغي حمايتها من وصول المستخدم.
- ويسمح للمستخدمين باسترجاع المعلومات الإحصائية عن السكان، مثل المتوسطات والمبالغ والحصص والحد الأقصى والحد الأدنى والانحرافات المعيارية.

- A population is a set of tuples of a relation (table) that satisfy some selection condition.
- Statistical queries involve applying statistical functions to a population of tuples.

- السكان هو مجموعة من صفوف العلاقة (الجدول) التي تلبي بعض شروط الاختيار.
- وتشمل الاستفسارات الإحصائية تطبيق وظائف إحصائية على مجموعة من الصفوف.

- For example, we may want to retrieve the *number* of individuals in a population or the *average income* in the population.
  - However, statistical users are not allowed to retrieve individual data, such as the income of a specific person.
- Statistical database security techniques must prohibit the retrieval of individual data.
- This can be achieved by prohibiting queries that retrieve attribute values and by allowing only queries that involve statistical aggregate functions such as COUNT, SUM, MIN, MAX, AVERAGE, and STANDARD DEVIATION.
  - Such queries are sometimes called statistical queries.

- على سبيل المثال، قد نرغب في استرداد عدد الأفراد في عدد السكان أو متوسط دخل السكان.
- ومع ذلك، لا يسمح للمستخدمين الإحصائيين لاسترداد البيانات الفردية، مثل دخل شخص معين.
- ويجب أن تحظر تقنيات أمن قاعدة البيانات الإحصائية استرجاع البيانات الفردية.
- ويمكن تحقيق ذلك من خلال حظر الاستعلامات التي تسترد قيم السمات والسماح فقط بالاستعلامات التي تتضمن وظائف إحصائية مجمعة مثل COUNT, SUM, MIN, MAX, AVERAGE, and STANDARD DEVIATION.
- وتسمى هذه الاستفسارات أحيانا الاستعلامات الإحصائية.

- It is DBMS's responsibility to ensure confidentiality of information about individuals, while still providing useful statistical summaries of data about those individuals to users. Provision of privacy protection of users in a statistical database is paramount.
- In some cases it is possible to infer the values of individual tuples from a sequence statistical queries.
  - This is particularly true when the conditions result in a population consisting of a small number of tuples.

- وتتحمل إدارة النظام مسؤولية ضمان سرية المعلومات عن الأفراد، مع توفير ملخصات إحصائية مفيدة للبيانات عن هؤلاء الأفراد إلى المستخدمين. توفير حماية الخصوصية للمستخدمين في قاعدة بيانات إحصائية أمر بالغ الأهمية.
- في بعض الحالات من الممكن استنتاج قيم فرادى الصفوف من الاستعلامات الإحصائية التسلسلية.
- وهذا صحيح بشكل خاص عندما تؤدي الظروف إلى عدد سكان يتكون من عدد قليل من الصفوف.

5 Introduction to Flow Control

- Flow control regulates the distribution or flow of information among accessible objects.
- A flow between object X and object Y occurs when a program reads values from X and writes values into Y.
  - Flow controls check that information contained in some objects does not flow explicitly or implicitly into less protected objects.
- A flow policy specifies the channels along which information is allowed to move.
  - The simplest flow policy specifies just two classes of information:
    - confidential (C) and nonconfidential (N)
  - and allows all flows except those from class C to class N.

- التحكم في التدفق ينظم توزيع أو تدفق المعلومات بين الأشياء التي يمكن الوصول إليها.
- يحدث تدفق بين الكائن X والكائن Y عندما يقرأ البرنامج القيم من X ويكتب القيم في Y.
- تتحقق ضوابط التدفق من أن المعلومات الواردة في بعض الكائنات لا تتدفق صراحة أو ضمنا في أشياء أقل حماية.
- وتحدد سياسة التدفق القنوات التي يسمح لها بنقل المعلومات.
- وتحدد أبسط سياسة تدفق فنتين فقط من المعلومات:
- سرية (C) وغير سرية (N)
- ويسمح لجميع التدفقات باستثناء تلك من الفئة C إلى الطبقة N.

5.1 Covert Channels

- A covert channel allows a transfer of information that violates the security or the policy.
- A covert channel allows information to pass from a higher classification level to a lower classification level through improper means.

- القناة سرية تسمح بنقل المعلومات التي تنتهك الأمن أو السياسة.
- وتسمح القناة السرية بالمرور من مستوى تصنيف أعلى إلى مستوى تصنيف أقل من خلال وسائل غير سليمة.

- **Covert channels** can be classified into two broad categories:
  - Storage channels do not require any temporal synchronization, in that information is conveyed by accessing system information or what is otherwise inaccessible to the user.
  - Timing channel allow the information to be conveyed by the timing of events or processes.
- Some security experts believe that one way to avoid covert channels is for programmers to not actually gain access to sensitive data that a program is supposed to process after the program has been put into operation.

- ويمكن تصنيف القنوات السرية إلى فنتين عريضتين:
- قنوات التخزين لا تتطلب أي تزامن زمني، في أن يتم نقل المعلومات عن طريق الوصول إلى معلومات النظام أو ما لا يمكن الوصول إليه على خلاف ذلك.
- قناة التوقيت تسمح بنقل المعلومات حسب توقيت الأحداث أو العمليات.
- ويعتقد بعض خبراء الأمن أن إحدى الطرق لتجنب القنوات السرية هي عدم تمكن المبرمجين من الوصول إلى البيانات الحساسة التي من المفترض أن يعالجها البرنامج بعد تشغيل البرنامج.

6 Encryption and Public Key Infrastructures

- **Encryption** is a means of maintaining secure data in an insecure environment.
- Encryption consists of applying an encryption algorithm to data using some prespecified encryption key.
- The resulting data has to be decrypted using a decryption key to recover the original data.

- التشفير هو وسيلة للحفاظ على بيانات آمنة في بيئة غير آمنة.
- يتكون التشفير من تطبيق خوارزمية التشفير على البيانات باستخدام بعض مفتاح التشفير المحددة مسبقاً.
- يجب أن يتم فك تشفير البيانات الناتجة باستخدام مفتاح فك تشفير لاستعادة البيانات الأصلية.

6.1 The Data and Advanced Encryption Standards

- The Data Encryption Standard (DES) is a system developed by the U.S. government for use by the general public.
  - It has been widely accepted as a cryptographic standard both in the United States and abroad.
- DES can provide end-to-end encryption on the channel between the sender A and receiver B.

- معيار تشفير البيانات (DES) هو نظام تم تطويره من قبل الحكومة الأمريكية لاستخدامه من قبل عامة الناس.
- وقد تم قبول على نطاق واسع كمعيار التشفير على حد سواء في الولايات المتحدة والخارج.
- DES يمكن أن يوفر التشفير من طرف إلى طرف على القناة بين المرسل A والمستقبل B.

- DES algorithm is a careful and complex combination of two of the fundamental building blocks of encryption:
  - substitution and permutation (transposition).
- The DES algorithm derives its strength from repeated application of these two techniques for a total of 16 cycles.
  - Plaintext (the original form of the message) is encrypted as blocks of 64 bits.

- خوارزمية DES هو مزيج دقيق ومعقد من اثنين من اللبنات الأساسية للتشفير:
- الاستبدال والتبديل (تبديل).
- خوارزمية DES تستمد قوتها من تطبيق المتكرر من اثنين من هذه التقنيات من مجموعه 16 دورات.
- يتم تشفير نص عادي (الشكل الأصلي للرسالة) كتل من 64 بت.

- After questioning the adequacy of DES, the National Institute of Standards (NIST) introduced the Advanced Encryption Standards (AES).
  - This algorithm has a block size of 128 bits and thus takes longer time to crack.

- بعد الإستطلاع في كفاءة DES، قدم المعهد الوطني للمعايير (NIST) معايير التشفير المتقدم (AES).
- هذه الخوارزمية لديها حجم كتلة 128 بت، وبالتالي يستغرق وقتا أطول للقضاء.

6.2 Public Key Encryption

- In 1976 Diffie and Hellman proposed a new kind of cryptosystem, which they called public key encryption.
- Public key algorithms are based on mathematical functions rather than operations on bit patterns.
  - They also involve the use of two separate keys
    - in contrast to conventional encryption, which uses only one key.
  - The use of two keys can have profound consequences in the areas of confidentiality, key distribution, and authentication.

- في عام 1976 اقترح ديفي وهيلمان نوعا جديدا من التشفير، الذي يسمى تشفير المفتاح العمومي.
- تستند خوارزميات المفاتيح العمومية إلى وظائف رياضية بدلا من العمليات على أنماط البتات.
- كما أنها تنطوي على استخدام مفتاحين منفصلين
- على النقيض من التشفير التقليدي، والذي يستخدم مفتاح واحد فقط.
- استخدام مفتاحين يمكن أن يكون له عواقب عميقة في مجالات السرية والتوزيع الرئيسي، والتوثيق.

- The two keys used for public key encryption are referred to as the public key and the private key.
  - the private key is kept secret, but it is referred to as private key rather than a secret key (the word used in conventional encryption to avoid confusion with conventional encryption).

- ويشار إلى المفتاحين المستخدمين لتشفير المفتاح العمومي بالمفتاح العمومي والمفتاح الخاص.
- يبقى المفتاح الخاص سريا، ولكن يشار إليه باسم المفتاح الخاص بدلا من المفتاح السري (الكلمة المستخدمة في التشفير التقليدي لتجنب الخلط مع التشفير التقليدي).

- A public key encryption scheme, or infrastructure, has six ingredients:
  - **Plaintext:** This is the data or readable message that is fed into the algorithm as input.
  - **Encryption algorithm:** The encryption algorithm performs various transformations on the plaintext.
  - **Public and private keys:** These are pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.
    - **The exec transformations** performed by the encryption algorithm depend on the public or private key that is provided as input.

- نظام تشفير المفتاح العمومي، أو البنية التحتية، لديه ستة مكونات:
- نص عادي: هذه هي البيانات أو الرسالة القابلة للقراءة التي يتم إدخالها في الخوارزمية كمدخلات.
- خوارزمية التشفير: تقوم خوارزمية التشفير بإجراء تحولات مختلفة على النص العادي.
- المفاتيح العامة والخاصة: هذه هي زوج من المفاتيح التي تم اختيارها بحيث إذا تم استخدام واحد للتشفير، ويستخدم الآخر لفك التشفير.
- تحولات إيكسيك التي تقوم بها خوارزمية التشفير تعتمد على المفتاح العام أو الخاص الذي يتم توفيره كمدخلات.

- A public key encryption scheme, or infrastructure, has six ingredients (contd.):
  - Ci**phertext:**
    - This is the scrambled message produced as output. It depends on the plaintext and the key.
    - For a given message, two different keys will produce two different ciphertexts.
  - **Decryption algorithm:**
    - This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

- يحتوي نظام تشفير المفتاح العمومي أو البنية التحتية على ستة مكونات (يتبع.):
- النص المشفر:هذه هي الرسالة التي يتم إنتاجها كمخرجات. ذلك يعتمد على النص العادي والمفتاح.
- بالنسبة إلى رسالة معينة، سيؤدي مفتاحان مختلفان إلى إنتاج نصين مختلفين.
- خوارزمية فك التشفير: تقبل هذه الخوارزمية النص المشفر ومفتاح المطابقة وتنتج النص العادي الأصلي.

- Public key is made for public and private key is known only by owner.
- A general-purpose public key cryptographic algorithm relies on
  - one key for encryption and
  - a different but related key for decryption.

- المفتاح العام مصنوع للمفتاح العام والخاص يعرفه المالك فقط.
- تعتمد خوارزمية تشفير المفتاح العمومي للأغراض العامة على
- مفتاح واحد للتشفير و
- مفتاح مختلف ولكن ذات الصلة لفك التشفير.

- **The essential steps are as follows:**
  - Each user generates a pair of keys to be used for the encryption and decryption of messages.
  - Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private (private key).
  - If a sender wishes to send a private message to a receiver, the sender encrypts the message using the receiver's public key.
  - When the receiver receives the message, he or she decrypts it using the receiver's private key.
    - No other recipient can decrypt the message because only the receiver knows his or her private key.

- والخطوات الأساسية هي كما يلي:
- كل مستخدم يولد زوج من المفاتيح لاستخدامها في التشفير وفك التشفير من الرسائل.
- يضع كل مستخدم أحد المفتاحين في سجل عام أو ملف آخر يمكن الوصول إليه. هذا هو المفتاح العمومي. يتم الاحتفاظ بمفتاح خاص (المفتاح الخاص).
- إذا رغب المرسل في إرسال رسالة خاصة إلى جهاز استقبال، يقوم المرسل بتشفير الرسالة باستخدام المفتاح العمومي للمستقبل.
- وعندما يستقبل المستقبل الرسالة، يقوم بتشفيرها باستخدام المفتاح الخاص للمستقبل.
- لا يمكن لأي مستلم آخر فك تشفير الرسالة لأن فقط المتلقي يعرف المفتاح خاص.

- The RSA **Public Key Encryption algorithm,** one of the first public key schemes was introduced in 1978 by Ron Rivest (R), Adi Shamir (S), and Len Adleman (A) at MIT and is named after them.
  - The RSA encryption algorithm incorporates results from number theory, such as the difficulty of determining the large prime factors of a large number.
- The RSA algorithm also operates with modular arithmetic – mod n, where n is the product of two large prime numbers.

- خوارزمية تشفير المفتاح العمومي RSA، وقد تم إدخال واحد من أول أنظمة المفاتيح العامة في عام 1978 من قبل رون ريفست (R)، آدي شامير (S)، ولين أدلمان (A) في معهد MIT، وسميت بعدهم.
- خوارزمية التشفير RSA يتضمن نتائج من نظرية العدد، مثل صعوبة تحديد العوامل الرئيسية الكبيرة لعدد كبير.
- خوارزمية RSA تعمل أيضا مع حساب وحدات ،نمطية الحساب حيث ن هو ناتج اثنين من الأعداد الأولية الكبيرة.

- **Two keys, d and e, are used for decryption and encryption.**
  - **An important property is that d and e can be interchanged.**
  - **n is chosen as a large integer that is a product of two large distinct prime numbers, a and b.**
  - **The encryption key e is a randomly chosen number between 1 and n that is relatively prime to (a-1) x (b-1).**
  - **The plaintext block P is encrypted as Pe mod n.**
  - **Because the exponentiation is performed mod n, factoring Pe to uncover the encrypted plaintext is difficult.**
  - **However, the decryption key d is carefully chosen so that (Pe)d mod n = P.**
  - **The decryption key d can be computed from the condition that d x e= 1 mod ((a-1)x(b-1)).**
  - **Thus, the legitimate receiver who knows d simply computes (Pe)d mod n = P and recovers P without having to factor Pe .**

- يستخدم مفتاحان، d و e، لفك التشفير والتشفير.
- خاصية هامة هي أن d و e يمكن أن تكون متبادلة.
- n هو عدد صحيح كبير هو ناتج رقمين رئيسيين متميزين كبيرين، أ و ب.
- ومفتاح التشفير e هو رقم يتم اختياره عشوائيا بين 1 و n يكون رئيسيا نسبيا إلى (a-1) x (b-1).
- يتم تشفير بلوك نص عادي Pe mod n.
- لأنه يتم تنفيذ mod n ، إلى Pe للكشف عن النص المشفر أمر صعب.
- ومع ذلك، يتم اختيار مفتاح فك التشفير d بعناية بحيث

(Pe)d mod n = P

- ويمكن حساب مفتاح فك التشفير d من الحالة

d x e= 1 mod ((a-1)x(b-1))

- وهكذا، فإن المتلقي الشرعي الذي يعرف d يحسب ببساطة (Pe)d mod n = P ويسترد P دون الحاجة إلى عامل pe.

6.3 Digital Signatures

- **A digital signature** is an example of using encryption techniques to provide authentication services in e-commerce applications.
- A digital signature is a means of associating a mark unique to an individual with a body of text.
  - The mark should be unforgettable, meaning that others should be able to check that the signature does come from the originator.
- A digital signature consists of a string of symbols.
  - Signature must be different for each use.
    - This can be achieved by making each digital signature a function of the message that it is signing, together with a time stamp.
  - Public key techniques are the means creating digital signatures.

- والتوقيع الرقمي مثال على استخدام تقنيات التشفير لتوفير خدمات التوثيق في تطبيقات التجارة الإلكترونية.
- التوقيع الرقمي هو وسيلة لربط علامة فريدة لفرد مع مجموعة من النص.
- يجب أن تكون العلامة لا تنسى، وهذا يعني أن الآخرين يجب أن تكون قادرة على التحقق من أن التوقيع لا يأتي من المنشئ.
- ويتألف التوقيع الرقمي من سلسلة من الرموز.
- يجب أن يكون التوقيع مختلفا لكل استخدام.
- ويمكن تحقيق ذلك من خلال جعل كل توقيع رقمي وظيفة للرسالة التي يتم التوقيع عليها، جنبا إلى جنب مع الطابع الزمني.
- وتقنيات المفاتيح العمومية هي الوسيلة التي تخلق التوقيعات الرقمية.

Summary

- 1 Database Security and Authorization
- 2 Discretionary Access Control
- 3 Mandatory Access Control and Role-Based Access Control for Multilevel Security
- 4 Statistical Database Security
- 5 Flow Control
- 6 Encryption and Public Key Infrastructures

وتم بحمد الله ..
وبالتوفيق للجميع ...