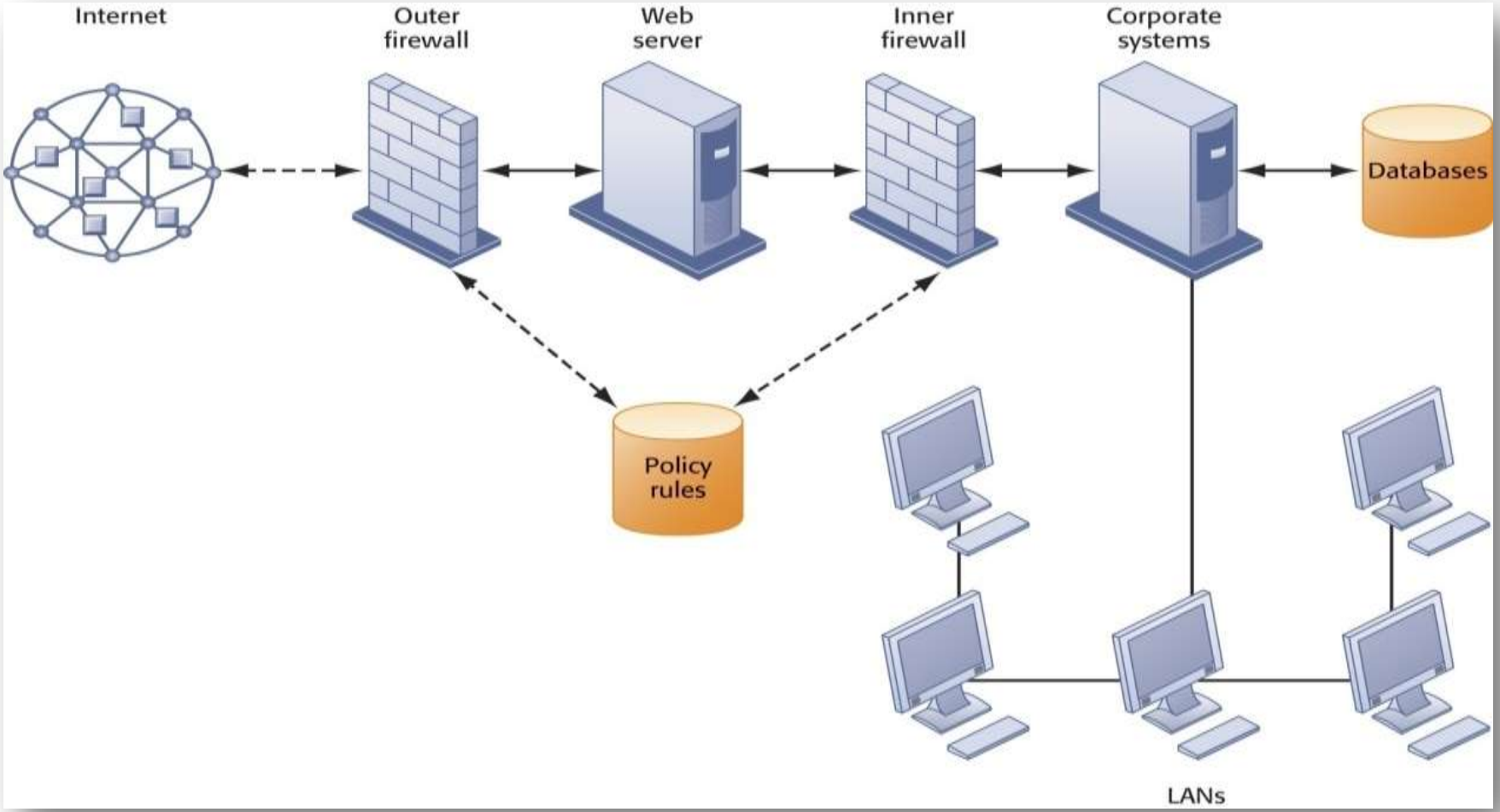
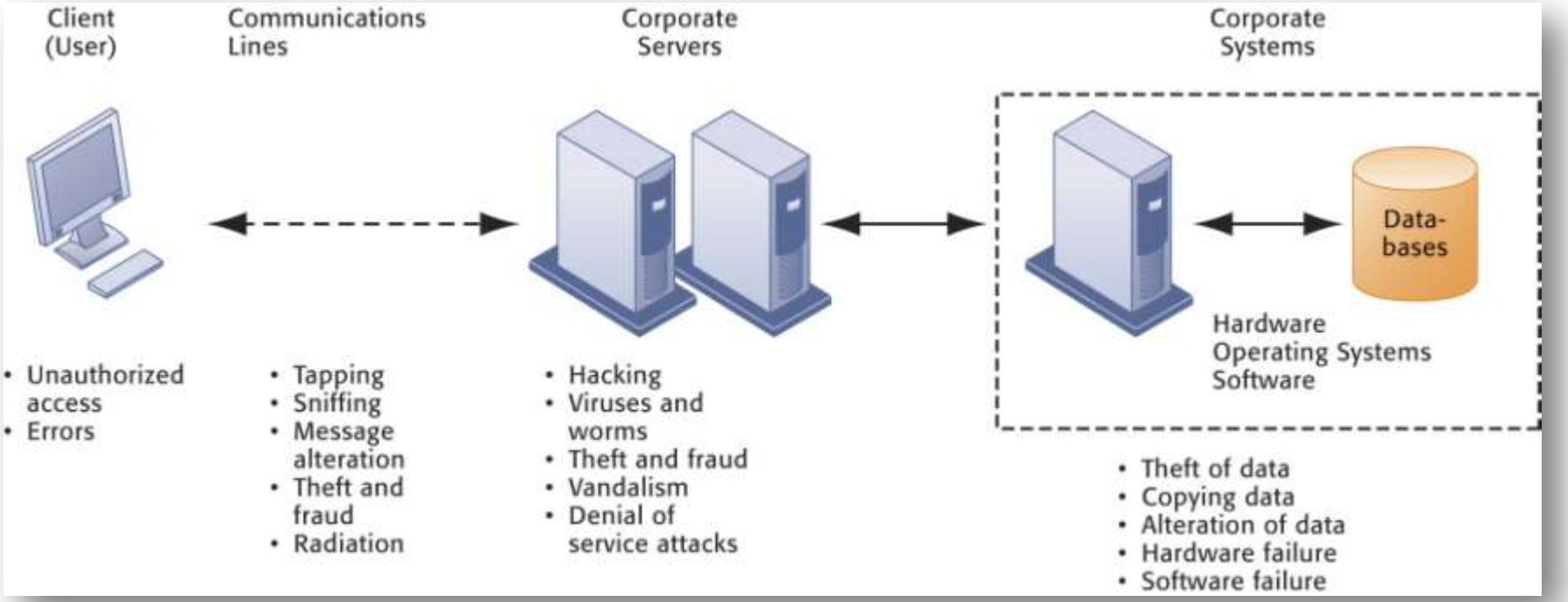
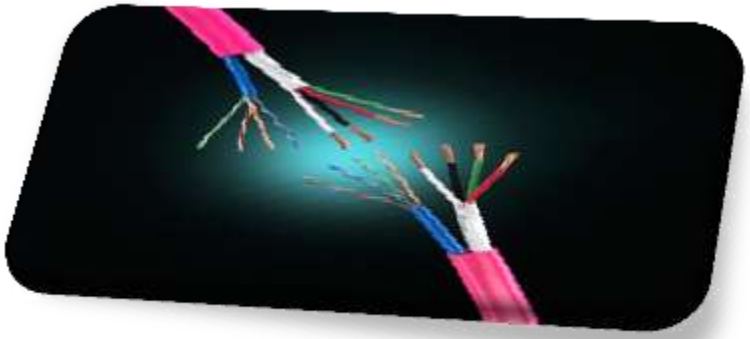
6

هيكلية الحكومة الإلكترونية

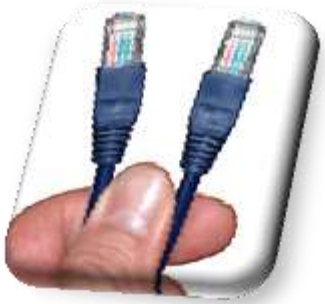
هيكلية شبكات الحاسوب

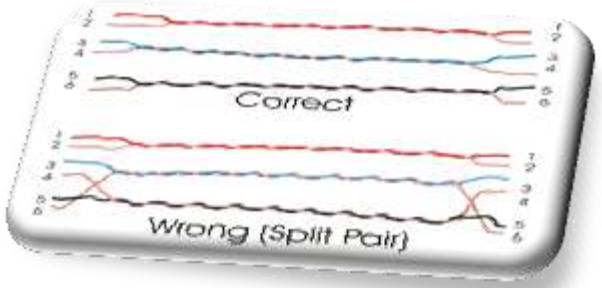


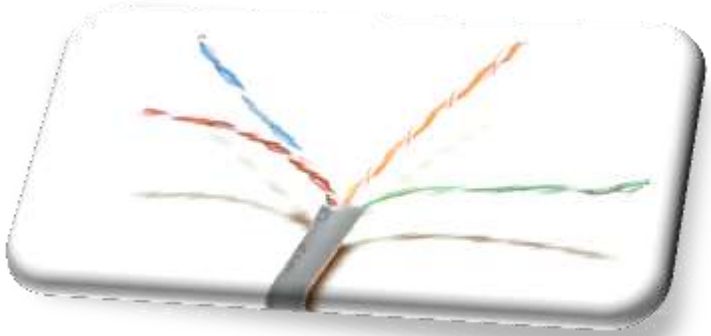

Client (User)
Communications Lines
Corporate Servers
Corporate Systems
Data-bases
Hardware
Operating Systems
Software
• Unauthorized access
• Errors
• Tapping
• Sniffing
• Message alteration
• Theft and fraud
• Radiation
• Hacking
• Viruses and worms
• Theft and fraud
• Vandalism
• Denial of service attacks
• Theft of data
• Copying data
• Alteration of data
• Hardware failure
• Software failure



الشبكة: مجموعة حواسيب متنوعة (طرفيات، حواسيب شخصية، محطات عمل، حواسيب متوسطة، حواسيب كبيرة وعملاقة) مرتبطة ببعضها البعض عن طريق وحدات ربط ووسائط (كوابل محورية، أسلاك مبرومة، ألياف ضوئية) وأجهزة ملحقة (أجهزة تقوية، مجمعات توصيل، جسر أو مسار ربط) مكونة بذلك شبكة متكاملة



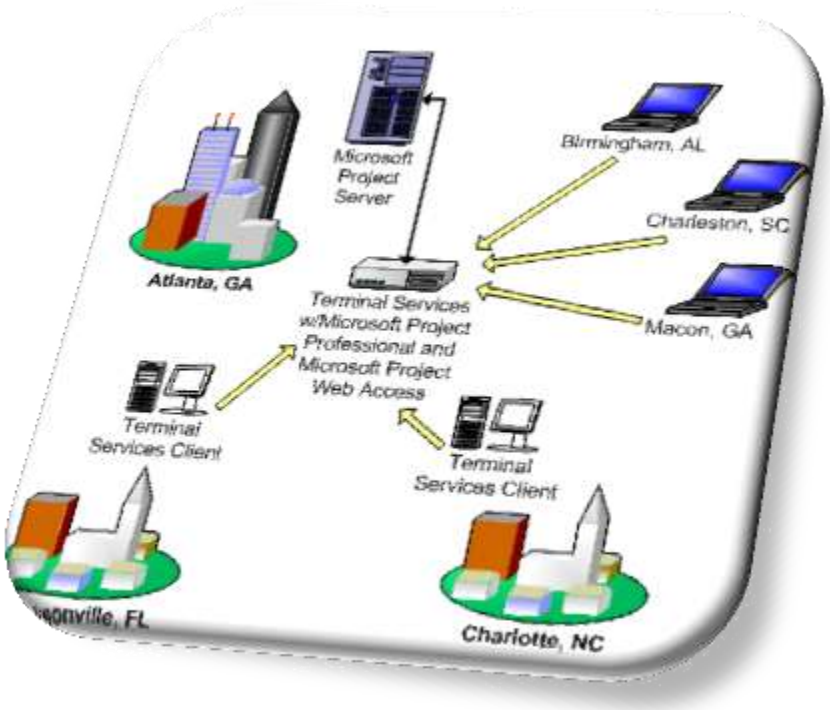




أنواع الشبكات

- ثلاثة أنواع رئيسية من الشبكات
- الشبكات الواسعة (WAN)
- الشبكات المحلية (LAN)
- الشبكات القطرية (MAN)

الشبكات الواسعة
Wide Area Network (WAN)



- شبكات تؤمن وصل مجموعة من الحواسيب الضخمة في مجموعة من الدول أو المناطق البعيدة
- يكون الربط بخطوط الهاتف والاتصال اللاسلكي
- مثال لهذا النوع الشبكة العنكبوتية العالمية (الانترنت)
- أنواع الشبكات الواسعة
- تنقسم شبكات الـــ WAN إلى فئتين:
- شبكات المؤسسات التجارية
- الشبكات العالمية

INTERNET

شبكات الحاسوب المحلية
Design LAN Network (LAN)

- أبسط أنواع الشبكات
- تتصل أجهزة الحاسوب عن طريق الكابلات
- أهم أنواع هذه الكابلات هو ما يسمى (Ethernet) تسمح بانتقال كمية لا بأس بها من المعلومات من خلال أجهزة الشبكة
- تسمح باتصالات سريعة بين الأجهزة ضمن نطاق الشبكة
- تحتوي على مئات من الأجهزة المتصلة مع بعضها ضمن مبنى أو مجموعة مباني متجاورة

Metro Area Network (MAN)
شبكات نطاق المدن

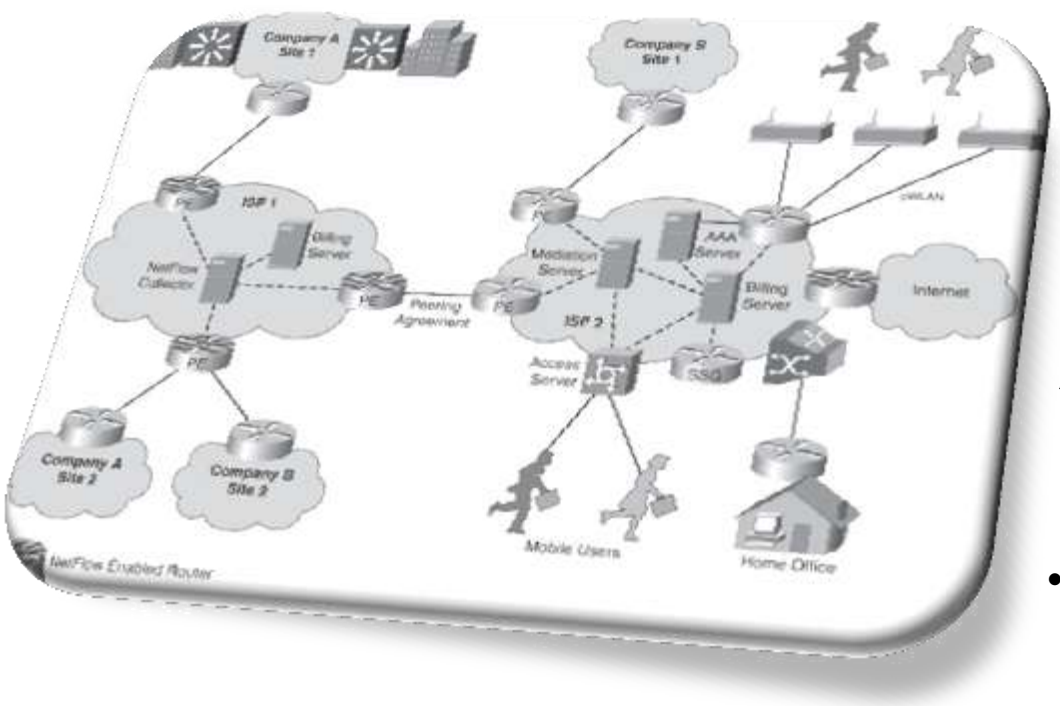
- تعتبر نوعاً آخر في تصنيف الشبكات
- تقوم على تكنولوجيا الشبكات المحلية
- تعمل بسرعة فائقة وتستخدم أليافاً ضوئية كوسط اتصال تغطي مساحة واسعة تتراوح بين 20 إلى 100 كيلومتر

أهداف شبكات الحواسيب

- المشاركة في الموارد المختلفة (معدات – برامج – بيانات)
- الحصول على بيانات ومعلومات من قواعد بيانات ومصارف معلومات في أماكن بعيدة
- نقل البيانات والمعلومات من مقدمي الخدمات إلى المستفيدين في جميع أنحاء العالم
- نقل البريد الالكتروني من مقدمي الخدمات وتوزيعها على المشتركين في أماكن مختلفة وبعيدة
- الإعتماد على حواسيب أخرى في حالة حدوث عطل أو خلل في بعض الحواسيب
- سرعة إنجاز تنفيذ عمليات معقدة بمشاركة أكثر من حاسوب

بعض المفاهيم حول
هيكيلة ربط الشبكات

التصاميم الأساسية للعمليات
Blueprint



- وصف للمكونات الأساسية للبنية التحتية اللازمة لتطبيق مشروع الحكومة الإلكترونية المقترحة للحكومة الإلكترونية
- تمثل هذه المكونات المواضيع الرئيسية الملموسة التي يجب مناقشتها من أجل تحقيق رؤية الحكومة الإلكترونية
- يمكن توضيح لبنات بناء التكنولوجيا الأساسية في الشكل الآتي

- **blueprint plan: program a series of steps to be carried out or goals to be accomplished**

إطار تداخل العمليات
Interoperability Framework

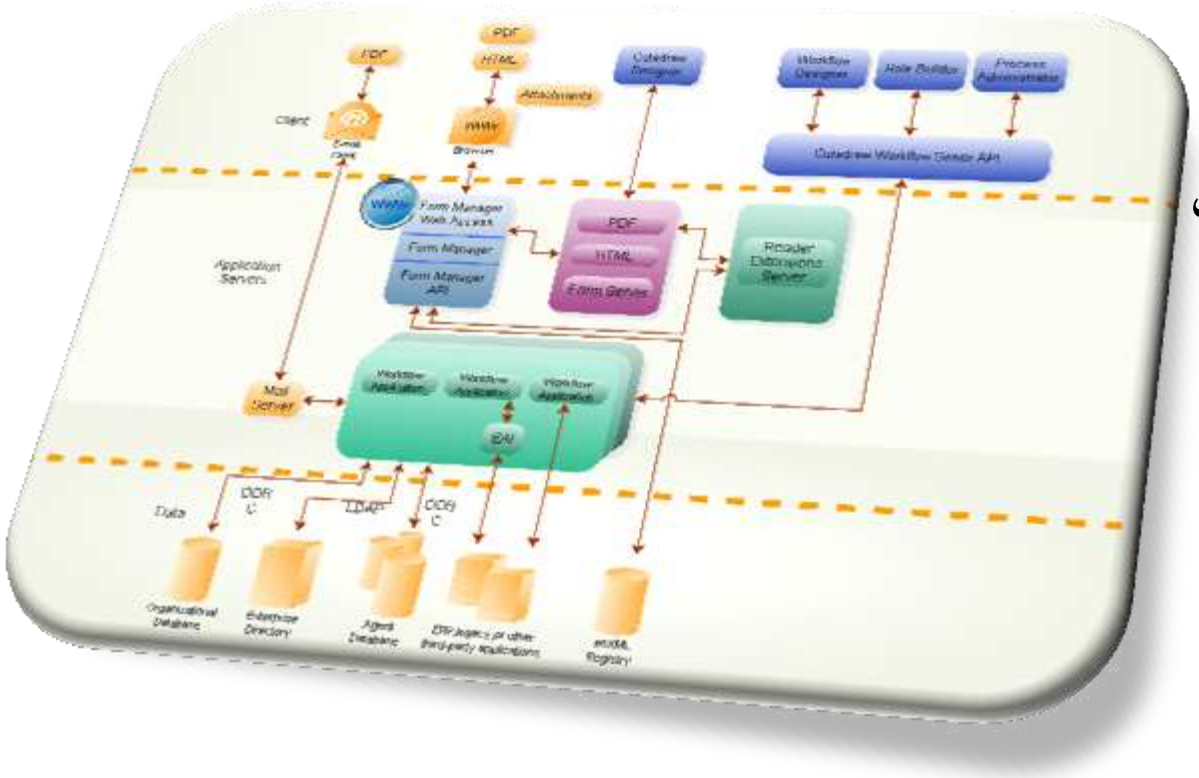
- تشمل العمليات، المعايير، القواعد، الأنظمة، التطبيقات اللازمة للحكومة الإلكترونية
- تداخل العمليات تستوجب منا التعامل مع عدد من القضايا الأساسية والتي تشمل:
  - اجراءات الاعمال الحكومية
  - سير العمل
  - المحتويات
  - ادارة الوثائق
  - معايير تداخل العمليات المعلوماتية
  - التطبيقات الرئيسية
  - اللغة
  - محرك البحث
  - بوابة الدفع الآلي

إجراءات العمل في الحكومة
Process Procedures

- تشمل إجراءات العمل اكثر من وزارة او دائرة حكومية، مما يتطلب القيام بإجراءات للتعامل ما بين الدوائر الحكومية الكترونيا يهدف إلى تحسين سرعة انجاز الاجراءات حيث يتم ارسال المعلومات المطلوبة مباشرة.
- لأن هدف الحكومة الإلكترونية "السرعة والكفاءة" فإن الحكومات تحتاج إلى توفر نوع من التدقيق على نتائج العمليات (بعد العملية)
- هذا النوع من التدقيق (بعد العملية) يؤدي إلى:
  - حذف الفحوصات التي تسبب بطء العمليات (إعادة هندسة الإجراءات)
  - تقليل عدد الدوائر الحكومية للعملية الواحدة

سير العمل

Work Flow



- سير العمل هو الطريقة التي يحددها النظام كمسار يسلكه المواطنين أثناء تنفيذ الإجراءات الحكومية
- يوجد نوعان من المحتوى:
  - المحتوى الثابت: يقدم معلومات عن الخدمات الحكومية
  - المحتوى المتغير: يسمح بإجراء التعاملات بين الحكومة وقطاع الاعمال وبين الحكومة والمواطنين

المعايير والنماذج
Standards and Forms

غالبا ما تكون نقطة البداية في أي جهاز حكومي "النماذج".
هنا يتوجب:

- ✓ تطوير المحتوى ونشره
- ✓ نشر التوجيهات بتصميم المواقع
- ✓ فصل عمليات التطوير، الفحص وتصميم الأنظمة
- ✓ فحص جميع تصاميم المواقع قبل السماح لها بالاتصال مع بوابة الشبكة
- ✓ إستمرار تحديث المحتويات
- ✓ ربط المعلومات الداخلية مع مواقع الشبكة
- ✓ تطوير معايير للمواقع
- ✓ تطوير سيناريوهات الفحص
- ✓ مراجعة جميع النماذج
- ✓ تطوير ادلة لتصميم النماذج
- ✓ تطوير اسلوب فحص النماذج
- ✓ النظر في امكانية طباعة النماذج وتوزيعها

معايير تداخل المعلومات
Information Interoperability Standards

- من أهم العناصرالاساسية لأي نظام حكومة إلكترونية هوتعريفها لمجموعة السياسات والمعايير العامة المتعلقة بتبادل أو إرسال الرسائل مابين الأطراف لمختلفة.
- من الضروري تعريفها ضمن وثيقة إطار (تداخل العمليات المعلوماتية) حيث يجب أن يحوي هذا الإطار تعريفا دقيقا للمعايير لكل من:
  - معايير تداخل الخدمات
  - معايير تكامل البيانات
  - معايير الوصول إلى المعلومات
- لا بد من إنشاء إطار عمل لتداخل العمليات وتحديد معايير لتداخل الخدمات وانتقال البيانات والوصول إلى المعلومات والتأكد بأن المعايير متاحة وقابلة للتطبيق ومرنة

محرك البحث

Search Engine

- يجب أن يتوفر باللغتين العربية والإنجليزية توفر للمستخدم أدوات البحث اللازمة عن الخدمات والمعلومات والعمليات على اي موقع تملكه الحكومة
- يجب أن تمكن محرك البحث للمستخدمين من القيام بتقديم طلبات الحصول على المعلومات بالعربية والإنجليزية على ان يتم حصرالبحث بمجالات الحكومة
- توفير البحث عن الكلمات والنصوص باللغة العربية والإنجليزية
- استخدام أسلوب الإشارات المتعاقبة زمنيا Meta tags للمساعدة على تصنيف المحتوى تطوير فهرس موحد لتسريع عملية البحث مراجعة الحاجة لتوفير قواعد بيانات لأكثر من لغة واحدة

- **Meta tags are HTML elements used to provide structured metadata**
- **about a web page. Such elements are placed as tags in the head**
- **section of an HTML document .**

الخدمات المشتركة

شبكة حكومية رئيسية آمنة (الإنترنت) لتوصيل أنظمة المعلومات في الدوائر والوزارات الحكومية المختلفة

- اتصالات داخلية ضمن دوائر ووزارات الحكومة
- مراكز معلومات آمنة (Data center)
- مركز المناداة (Call center)

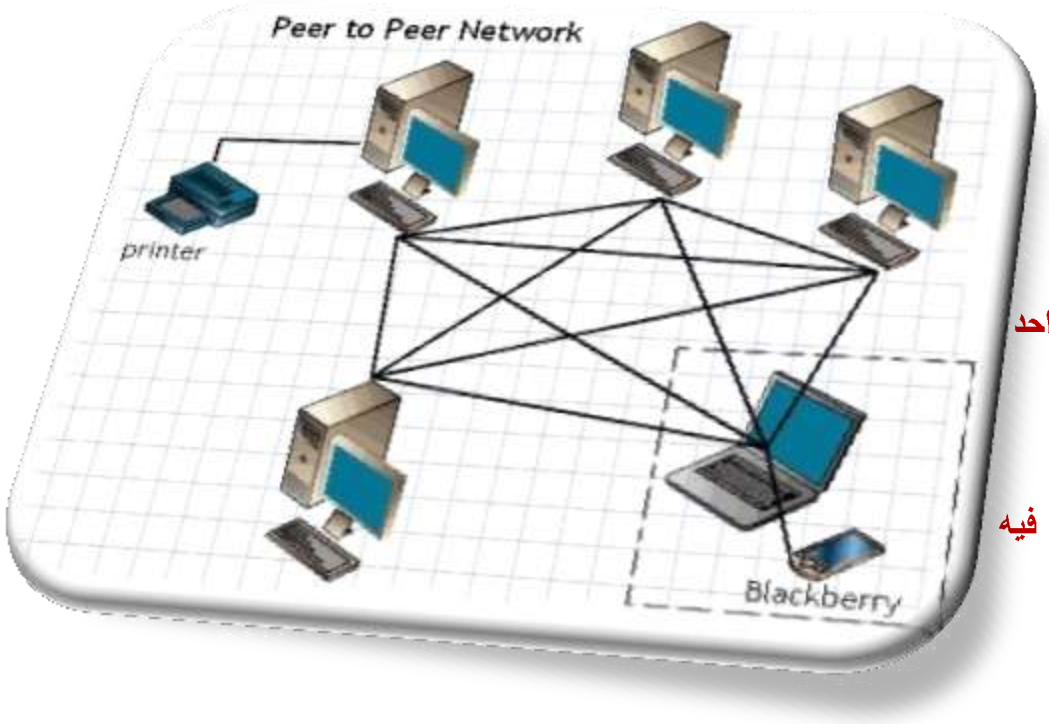
إدارة المعرفة

Knowledge Management

- **إمكانية توصيل المطالبات وردودها بين المواطن والحكومة**
- **القيام بذلك بسرية تامة وموثوقية عالية هي الأساس لأي مشروع حكومة إلكترونية على الإطلاق ومن خلال البوابة الرئيسية**
- **التكنولوجيا الرئيسية التي يمكن استخدامها في تبادل الرسائل هي الهاتف، الفاكس، البريد الإلكتروني**
- **البريد الإلكتروني:** وسيلة تكنولوجية جديدة في مجال تبادل الرسائل و لها فوائد مثل ملائمتها لرغبة المستلم، وصول الرسائل بسرعة أكثر من التقليدية موثقة أكثر من المكالمة الهاتفية، يمكن توزيعه على عدة مستقبلين في آن واحد

الشبكات المتكافئة

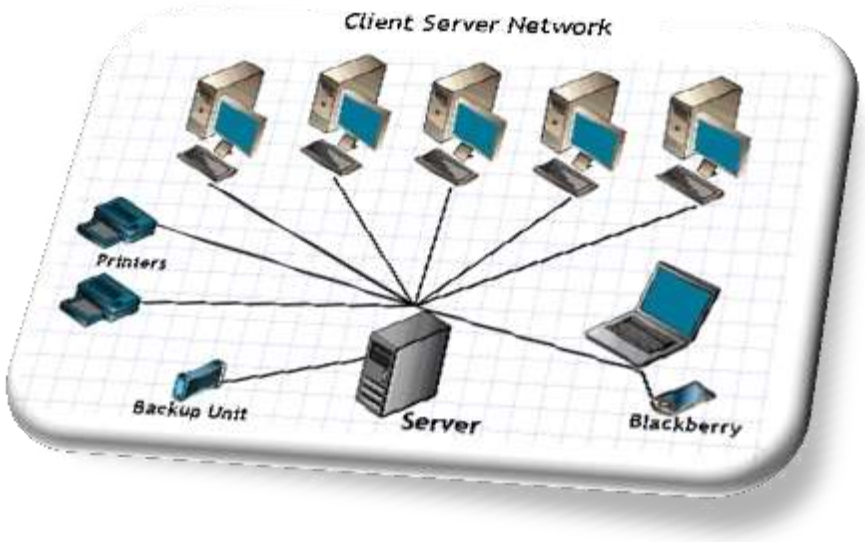
Peer to Peer Networks



- **مزايا الشبكات المتكافئة**
- لا تحتاج إلى برامج إضافية على نظام التشغيل
- لا تحتاج إلى أجهزة ذات قدرات عالية
- سهلة التثبيت
- تكلفتها قليلة
- عالية التوثيق

- **عيوب الشبكات المتكافئة**
- فعالية الشبكة ترتبط بعدد المحطات التي تعمل في آن واحد
- صعوبة تنظيم التحكم الفعال بين المحطات
- صعوبة تحديث وتبديل محطات العمل
- غير مناسبة للشبكات الكبيرة
- عدد الأجهزة في الشبكة لا يتجاوز العشرة
- ضرورة تواجد المستخدمين في نفس المكان الذي توجد فيه الشبكة
- عدم أهمية أمن الشبكة
- عدم وجود خطط لتنمية الشبكة وتطويرها في المستقبل القريب

شبكات المزود / الزبون
Client / Server Network



تتميز بـــ:

- **إمكانية النسخ الاحتياطي للبيانات وفق جدول زمني محدد**
- **حماية البيانات من الفقدان والتلف**
- **تدعم آلاف المستخدمين**
- **تزيل الحاجة إلى الأجهزة القوية**
- **موارد الشبكة متمركزة في مزود واحد مما يسهل الوصول إلى المعلومات المطلوبة**

سيناريوهات تحقيق الحكومة الإلكترونية

- تم بناء حكومات الكترونية ناجحة في اماكن مختلفة من العالم باستخدام انواع عديدة من التكنولوجيا مما نتج عنها تحسين اداء الخدمات الحكومية باستخدام الفاكس والهاتف وتكنولوجيا اخرى
- مازالت نسبة انتشار الإنترنت في الدول العربية قليلة وبالتالي يجب عدم حصر طريقة تقديم خدمات الحكومة الإلكترونية بالإنترنت فقط ويمكن استخدام الإنترنت في نشر المعلومات
- من العوامل الاساسية للنجاح في نشر المعلومات هو استخدام البوابات التي تقوم بالتعرف على المستخدمين وتمييزهم وتقديم خدمات موحده لمستخدمي الشبكة

السيناريو(1) تكنولوجيا الفاكس والهاتف

- تناسب التكنولوجيا تلك الدول التي تفتقر الي بنية اتصالات تحتية او الحالات التي لا يستطيع الموطنون الحصول على التدريب الفني يمثل الهاتف والفاكس فرصة لبدء إستخدام الحكومة الإلكترونية دون الحاجة لإستثمارات عالية إضافه الى ضرورة توفر امكانية ضمان وصول أي وثيقة او التأكد من استلامها والحالة التي وصلت بها الوثيقة

السيناريو(2): تكنولوجيا الحواسيب والأكشاك

- تعتمد العديد من الحكومات على استخدام الإنترنت في تطبيق الحكومة الإلكترونية
- ويتطلب استثمارات عالية كأجهزة توصيل للمستخدمين لتكون شبكة حكوميه امنه لتوصيل الدوائر الحكومية فيما بينهم
- وتقديم التدريب المناسب لموظفي الحكومة

سيناريو(3): الوسيط بين السيناريو الأول والثاني

- يجمع السيناريو الثالث بين اسلوب الانترنت والهاتف والفاكس بطريقة تناسب حاجة المستخدم الفردي
- يسمح الاسلوب للحكومات باستخدام ما هو متوفر من التكنولوجيا التي تعتمد على الهاتف لكي تكسب الخبرة اللازمة وتعمل على تأسيس مجموعة من المواطنين دائمي الاستخدام للتكنولوجيا

اتصال

حواسيب شخصية في المؤسسات

اكشاك إلكترونية في المراكز العامة

حواسيب شخصية في المنازل

أجهزة الهاتف النقال

نقاط اتصال اخرى

الإنترنت

وابة

البوابة وإدارة المحتويات

شتركة

تحويل البيانات

تبادل الرسائل

التعرف على المستخدم والدخلاء

آلية المعاملات وسير العمل

وظائف التدقيق والإدارة

أنظمة الدفع

المؤسسات المالية الخارجية

دائرة حكومية أ

دائرة حكومية ب

عناصر هامة غير ملموسة تمثل مجالات مهمة للحكومة الإلكترونية

- سياسة أمنية شاملة لجميع الدوائر والوزارات
- وحدة التقييم وترخيص مسئولة عن وضع السياسة الأمنية
- فريق تدريب مخصص لتدريب موظفي الحكومة فريق دعم مخصص لتقديم الإستشارات وللتدريب للمستخدمين من مواطنين وعاملين في القطاع الخاص
- سياسة موحدة التعامل مع المواضيع مثل تطوير الأنظمة التطبيقية

الإعتبارات العامة

المعايير الأمنية (Security Standards): مجموعة من السياسات والمعايير العامة المتعلقة بالأمن تشمل الشبكة الفعلية وأمن الأنظمة والبيانات وأسلوب الصلاحيات والوصول إلى المعلومات الشخصية

الخصوصية (Privacy): تخزين البيانات عن الأفراد وعاداتهم في استخدام الشبكة والمواقع. ومن الضروري وجود أسلوب السماح للمستخدمين للتأكد من أية معلومات شخصية لايتم تقديمها إلا من خلال الأشخاص الذين لهم صلاحية الوصول إليها

الإنتشار والترويج: لجعل المواطنين يشعرون بوجود الخدملات على الشبكة وللتأكد بأن توقعات المواطنين قد تم تحقيقها. (مدى انتشار استخدام الحواسيب الشخصية للإنترنت، مستوي مهارات التجارة الإلكترونية للمواطنين وللعاملين في الحكومة، بناء علاقات مع الصحافة

الدعم: تطوير آلية الدعم لإجراءات: حكومة – قطاع الاعمال،حكومة –مواطن، قطاع الأعمال – حكومة، مواطن حكومة

التعليم: المستوى العام لثقافة استخدام الإنترنت والحواسيب الشخصية من أهم العوامل التي تؤثر في نشر التجارة الإلكترونية. التعريف بالمفاهيم الضرورية لتمكين المواطنين من مناقشة فوائد المجتمع الإلكتروني.

المتطلبات القانونية: غالبية الحكومات العربية قد أنشأت إطارا قانونيا جديدا للتجارة الإلكترونية لكن هذا القانون مازال بإنتظار المصادقة عليه

7

التحديات الأمنية للحكومة الإلكترونية

الحكومة الالكترونية وتحديات الأمان

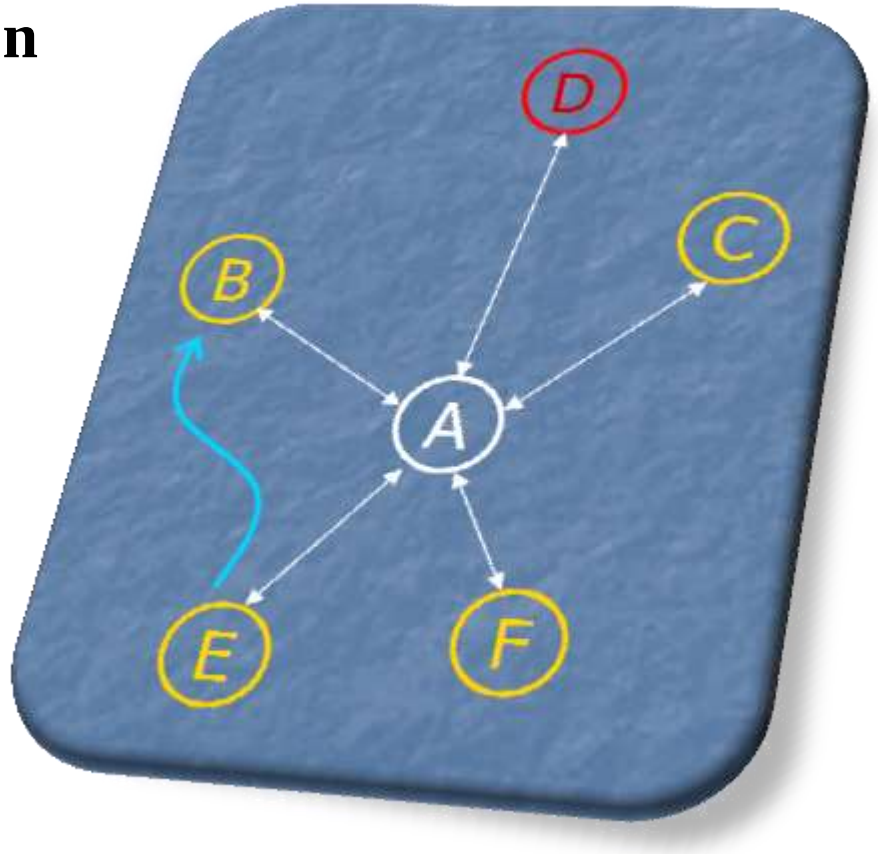
التحديات تكمن في:

- خصوصية المعلومات Privacy : بحيث لايتمكن من مشاهدتها إلا صاحب الرسالة عن طريق استخدام كلمات المرور والجدار الناري وشهادات الترخيص
- سلامة المعلومات Integrity: وذلك لحماية نقل المعلومات وتخزينها وأي تغيير متعمد وأي عبث بشري ضد تلف وتشويه الملفات ولتلافي ذلك يمكن استخدام البصمة الالكترونية والتشفير وبرامج مضادة الفيروسات واستخدام نماذج احتياطية
- التحقق من هوية الأطراف الأخرى Peer Authentication : وذلك لتجنب أي شكل من أشكال الخداع وللتحقق من ذلك لابد من التحقق من كلمات المرور والتواقيع الرقمية وبصمة الأصابع لدى الأطراف المتصلة

خصوصية المعلومات
Privacy

سلامة المعلومات
Integrity

التحقق من هوية الأطراف الأخرى
Peer Authentication



Authentication of the peer A through the trusted group of B. E sends an authentication vote to B, and D is a malicious peer.

طبيعة المخاطر الإلكترونية وأنواعها

- المواطن: من لديه الحق في الدخول الى بوابة الحكومة
- الموظف: الذي لديه الحق في دخول الشبكة الإلكترونية والإطلاع على الأنظمة
- المخابرات الصديقة والعدوة: إختراق النظام الأمني المعلوماتي ومختلف الأنظمة
- خطر المؤسسات التجارية بهدف المنافسة
- خطر المنظمات الإرهابية (الحرب الإلكترونية)
- خطر مزودي البرمجيات والتجهيزات الإلكترونية
- خطر الكوارث الطبيعية (الزلازل، الحرائق، الصواعق)
- خطر عيوب التصميم والتشغيل
- خطر تناثر وتنوع تطبيق مفاهيم الأمن والسرية عبر الإدارات
- خطر عدم الوعي بالمخاطر وعدم وضع خطط الدفاع والطوارئ

الأساليب التي يتبعها مخترقوا الأنظمة

عن طريق الحصول على صلاحيات المسئول عنه

عن طريق الموظف الذي يغضب من شركته يقوم بالإنتقام من منها

إغراق ذاكرة buffer وهو أسلوب هجوم شائع الاستغلال

الهجوم على لب النظام و تثبيت برمجيات في لب النظام بغرض السيطرة على أوامر النظام والدخول إلى البيانات

ثغرات أمنية في التطبيقات Bugs وهذا يعتبر من الأخطاء الشائعة في أي حاسوب نظرا لتزايد سرعة سوق تطبيقات الأعمال الاليكترونية

نصوص (cgi) المليئة بالأخطاء بطبيعتها وتتضمن ثغرات أمنية يمكن استخدامها في مهاجمة الويب

تشمم كلمات السر Sniffing: يعتبر من أساليب المخترقون حيث يقومون بمحاولة تخمين كلمات السر لمستخدمين شرعيين أو باعتراض طريق كلمات السر أثناء انتقالها عبر الشبكات

الخطأ الانساني وتتم خلال انتحال شخصية الموظفين داخل الشركات الخاصة بتقنية المعلومات

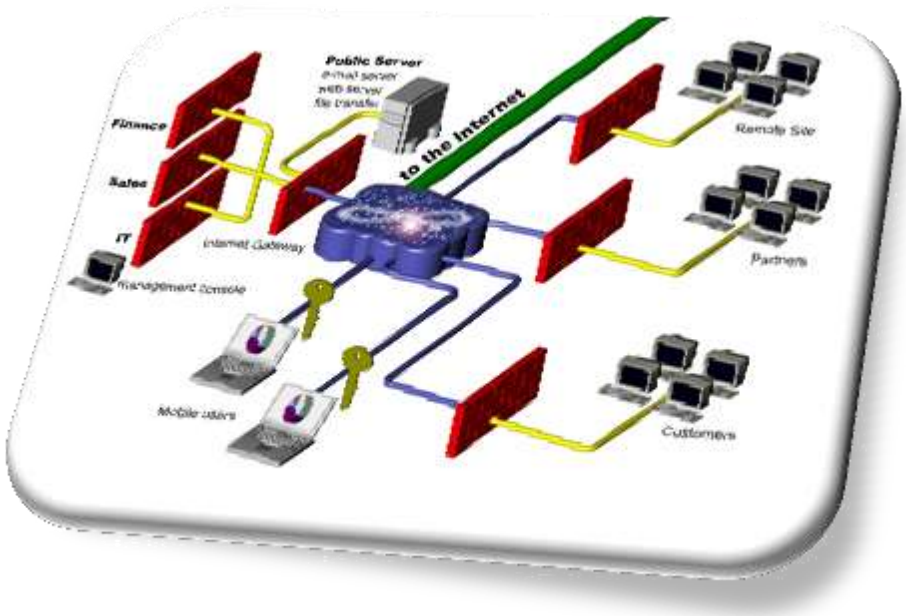
الفيروسات وحصان طروادة Backdoors وهي برامج تزرع خلسة وصممت لتنفيذ هجمات لتسبب التدمير ويطلق عليها الأبواب الخلفية

رفض الخدمة Denial of Service وفي هذا النوع يتم إغراق الحاسوب الخادم بسيل من الطلبات المزورة تسبب في إغلاق الجهاز أو إبطاء عمله

وسائل حماية الحكومة الالكترونية

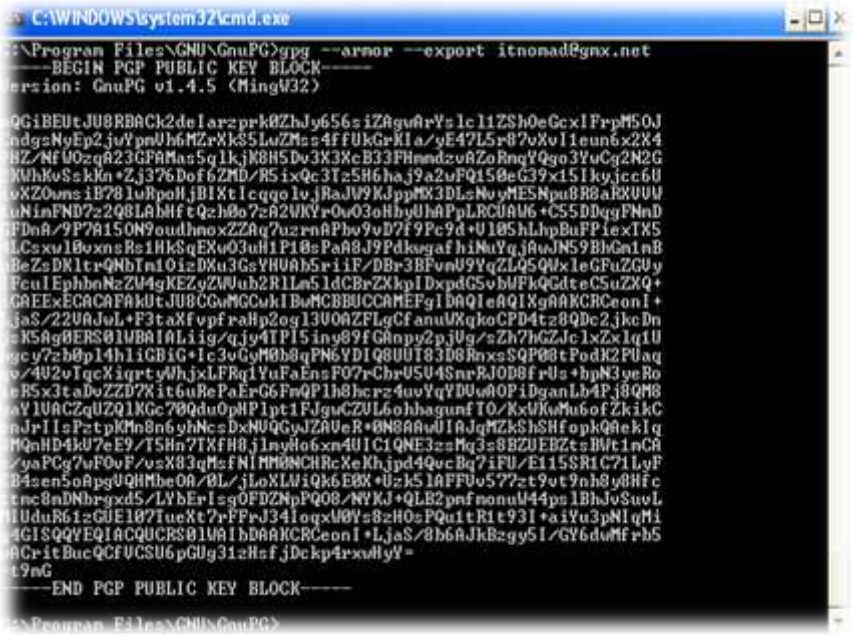
التشفير

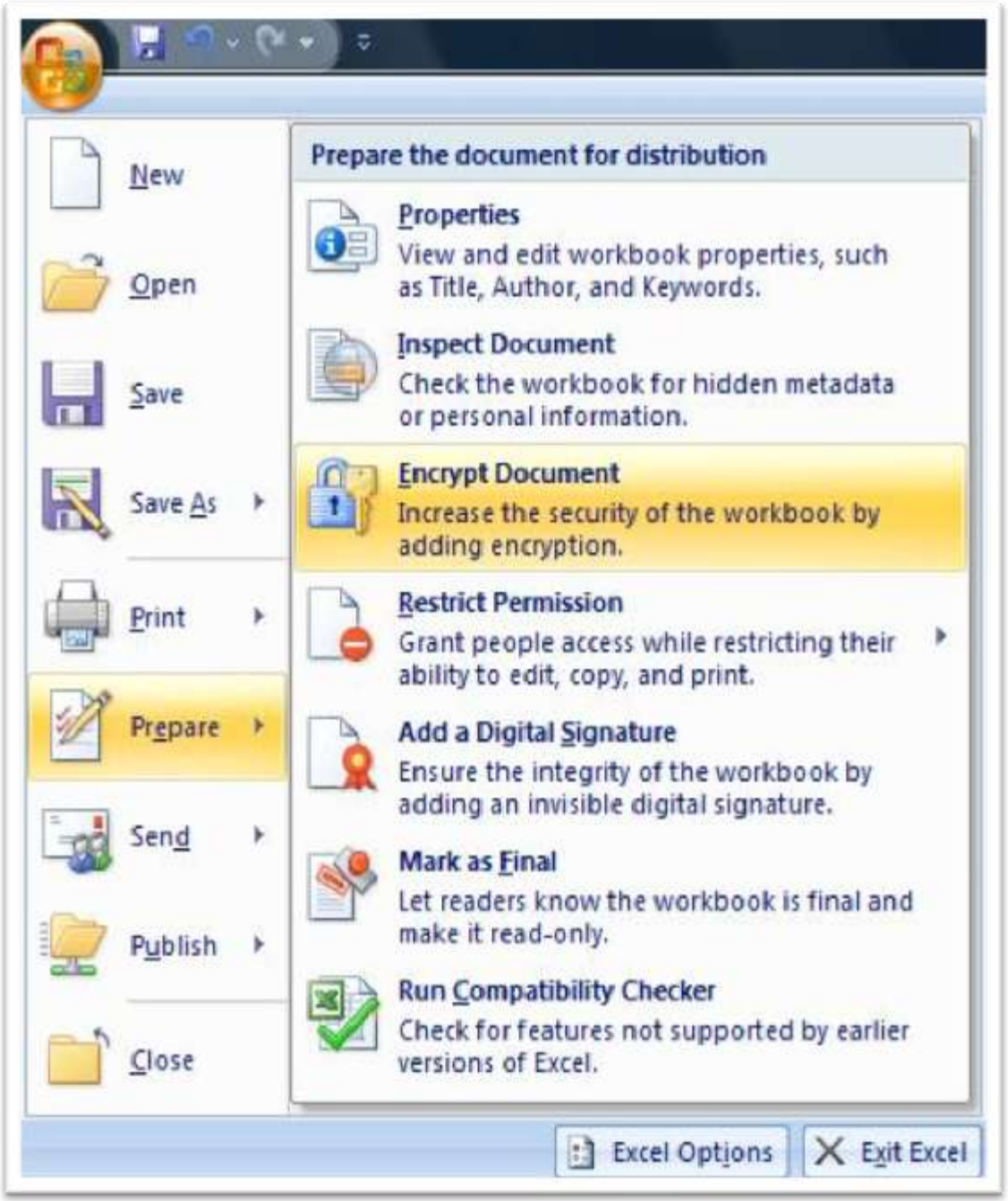
- يعرف بأنه عملية تحويل المعلومات إلى شفرات غير مفهومة لمنع الأشخاص الغير المرخص لهم من الاطلاع على المعلومات تنطوي تحت عملية تحويل النصوص العادية إلى نصوص مشفرة
- عوامل قوة وتأثير عملية التشفير
  - الخوارزمية
  - طول المفتاح مقدر بالبت



أنواع التشفير

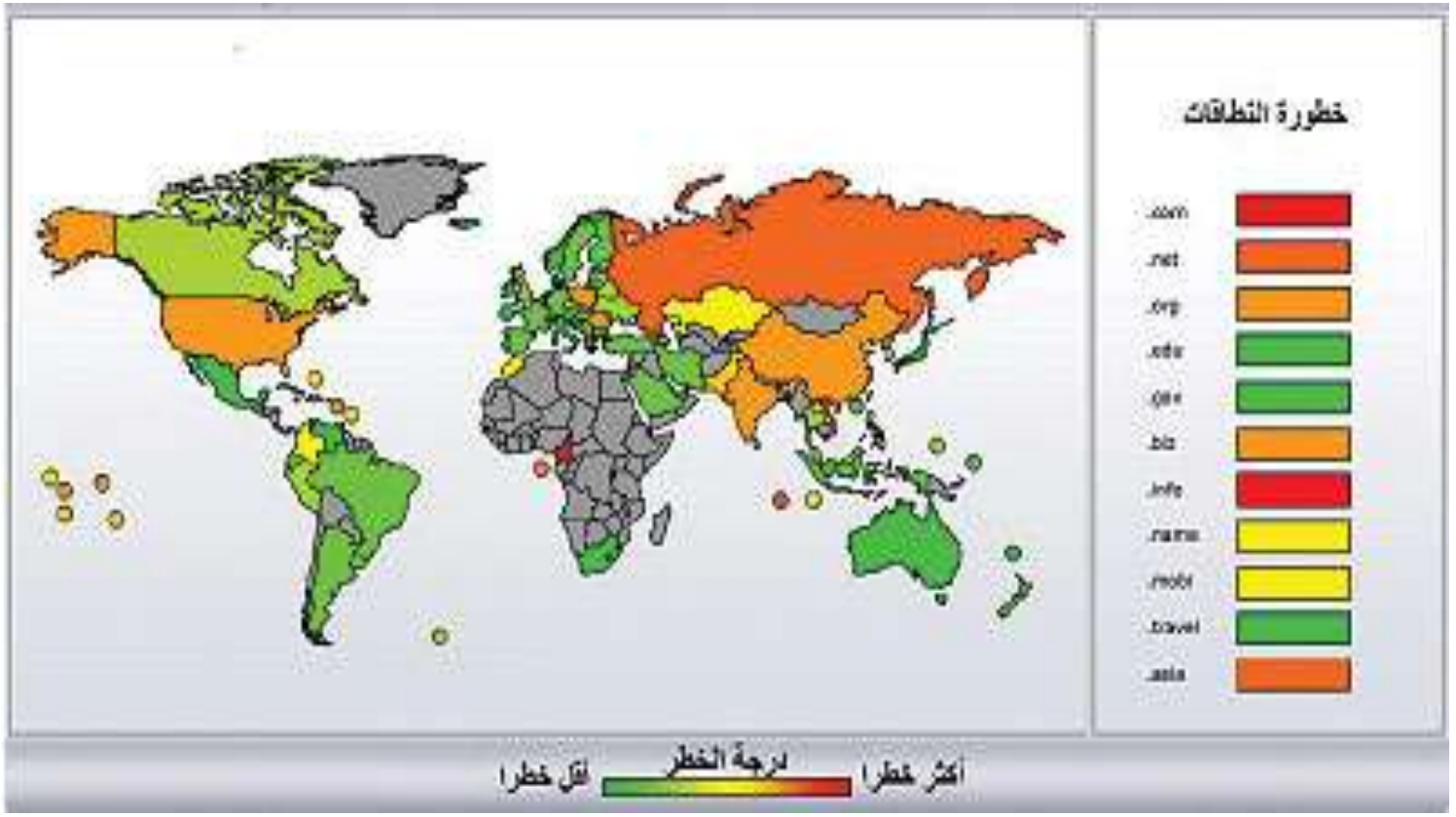
- التشفير المتماثل: وفيه يستخدم كل من المرسل والمستقبل المفتاح السري ذاته في تشفير الرسالة وفك تشفيرها ويتفق الطرفان في البداية على عبارة مرور التي سيتم استخدامها
- التشفير اللا متماثل (المفتاح العام): جاء حلا لمشكلة التوزيع غير الآمن للمفاتيح في التشفير المتماثل حيث يستخدم مفتاحان بدلا من مفتاح واحد




New
Open
Save
Save As
Print
Prepare
Send
Publish
Close
Prepare the document for distribution
Properties
View and edit workbook properties, such as Title, Author, and Keywords.
Inspect Document
Check the workbook for hidden metadata or personal information.
Encrypt Document
Increase the security of the workbook by adding encryption.
Restrict Permission
Grant people access while restricting their ability to edit, copy, and print.
Add a Digital Signature
Ensure the integrity of the workbook by adding an invisible digital signature.
Mark as Final
Let readers know the workbook is final and make it read-only.
Run Compatibility Checker
Check for features not supported by earlier versions of Excel.
Excel Options
Exit Excel


About
Picture Encryption
Register
Buy
OK

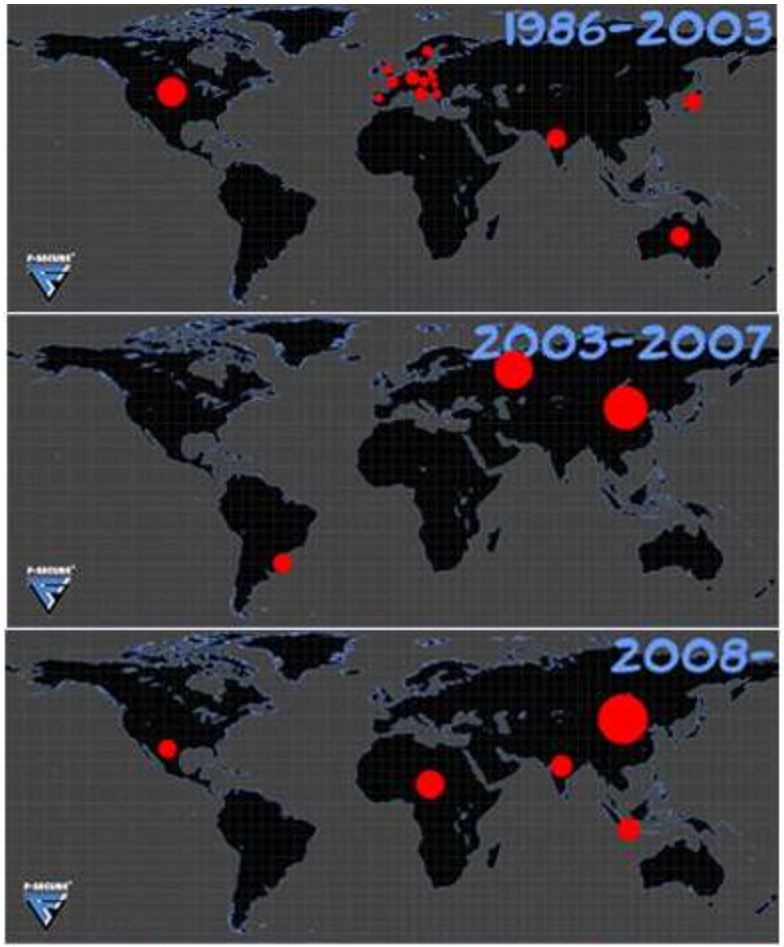
أخطر التهديدات الإلكترونية.. تحديات تمتحن الأمن الرقمي حول العالم



الثلاثـــاء 25 ذو القعـــدة 1431 هـــ 2 نوفمبر 2010 العدد 11662

الشرق الأوسط

الجريمة الإلكترونية فى تطور دائم ويجب إعادة تفصيل التشريعات من وقت لآخر



The Past, Recent History and Future of Internet Crime

البصمة الإلكترونية

- البصمة الإلكترونية للرسالة تدل على اقترانات تمويه حيث تطبق هذه الخوارزميات بحسابات رياضية على الرسالة لتوليد بصمة ملحوظة
- من غير الممكن اشتقاق البصمة الالكترونية من رسالتين مختلفين وتتميز بحسب أنواع مفاتيحها العامة والخاصة وتعتبر أسرع بكثير من نظام التشفير اللا متماثل

التوقيع الرقمي

ويستخدم للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل ويتم تأمين سلامة الرسالة والتحقق من صحتها ويمنع المرسل من التنكر للمعلومات التي أرسلها وتتم عن طريق دمج البصمة الالكترونية مع تشفيرها بمفتاح خاص

التوقيع الإلكتروني

- ملف رقمي صغير (شهادة رقمية) تصدر عن الهيئات المتخصصة والمستقلة ومعترف بها من الحكومة
- في هذه الملفات يتم تخزين الاسم وبعض المعلومات المهمة الأخرى مثل رقم التسلسل وتحتوي عند تسليمه على مفتاحين (مفتاح عام , مفتاح خاص)

حقائق عن التوقيع الإلكتروني

شهادة رقمية تصدر عن الهيئات المستقلة لتمييز كل مستخدم على حدة

تعتبر الوثائق والعقود المذيلة بالتوقيع الإلكتروني لاتحتاج إلى مصادقة من كاتب عدل أو أي جهة أخرى لاتستطيع استخدامها في القضايا المدنية ولا الإجرامية

كيفية الحصول على توقيعك الإلكتروني

- التقدم لإصدار الشهادات
- يتم إصدار الشهادة ومعها المفتاح العام والخاص
- تقوم أنت بتشفير الرسالة باستخدام المفتاح العام الخاص بالمستقبل أو الخاص بك
- يقوم البرنامج الخاص بالمستقبل ارسال نسخة من التوقيع الإلكتروني إلى الهيئة التي أصدرت الشهادة للتأكد من صحة التوقيع
- تقوم أجهزة الحاسوب المتخصصة في مراجعة قاعدة البيانات الخاصة بها ويتم التعرف على صحة التوقيع وتعاد النتيجة
- يتم إرسال المعلومات والنتيجة إلى المستقبل مرة أخرى للتأكد من صحة وسلامة الرسالة
- يقوم المستقبل بقراءة الرسالة وذلك عن طريق استخدام المفتاح الخاص به

الشهادات الرقمية

- طورت شركة نتسكيب بروتوكول الطبقات الأمنية لتأمين نقل المعلومات بين خادم الويب ومستعرضات الويب ويعتمد على خوارزمية المفتاح العام والمفتاح الخاص إذ يستطيع المستفيد بإنشاء زوج من المفاتيح العامة والخاصة لإرسال المعلومات إلى الخادم وفي الوضع الآمن يقوم الشخص بتوليد زوج من المفاتيح العامة / الخاصة ثم يرسل المفتاح العام إلى جهة مانحة للشهادة (CA) وتضيف الجهة بعض المعلومات المتعلقة بالشهادة ويوقع عليها بالمفتاح العام لطلب الشهادة ويصادق عليها المفتاح العام للشهادة ثم ترسل إلى صاحبها

Public-key cryptography

- A big random number is used to make a public-key/private-key pair.
- Anyone can encrypt using the public key, but only the holder of the private key can decrypt. Secrecy depends on the secrecy of the private key.
- Using a private key to encrypt (thus signing) a message; anyone can check the signature using the public key. Validity depends on private key security.
- By combining your own private key with the other user's public key, you can calculate a shared secretthat only the two of you know. The shared secret can be used as the key for a symmetric cipher.
- Public-key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys - apublic key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.
- Conversely, secret key cryptography, also known as symmetric cryptographyuses a single secret key for both encryption and decryption.
- The two main branches of public key cryptography are:
- Public key encryption — a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality.
- Digital signatures — a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This is used to ensure authenticity.
- An analogy for public-key encryption is that of a locked mailbox with a mail slot. The mail slot is exposed and accessible to the public; its location (the street address) is in essence the public key. Anyone knowing the street address can go to the door and drop a written message through the slot; however, only the person who possesses the key can open the mailbox and read the message.
- An analogy for digital signatures is the sealing of an envelope with a personal wax seal. The message can be opened by anyone, but the presence of the seal authenticates the sender.
- A central problem for public-key cryptography is proving that a public key is authentic, and has not been tampered with or replaced by a malicious third party. The usual approach to this problem is to use apublic-key infrastructure (PKI), in which one or more third parties, known as certificate authorities, certify ownership of key pairs. Another approach, used by PGP, is the "web of trust" method to ensure authenticity of key pairs.
- Public key techniques are much more computationally intensive than purely symmetric algorithms. The judicious use of these techniques enables a wide variety of applications. In practice, public key cryptography is used in combination with secret-key methods for efficiency reasons. For encryption, the sender encrypts the message with a secret-key algorithm using a randomly generated key, and that random key is then encrypted with the recipient's public key. For digital signatures, the sender hashes the message (using a cryptographic hash function) and then signs the resulting "hash value". Before verifying the signature, the recipient also computes the hash of the message, and compares this hash value with the signed hash value to check that the message has not been tampered with.

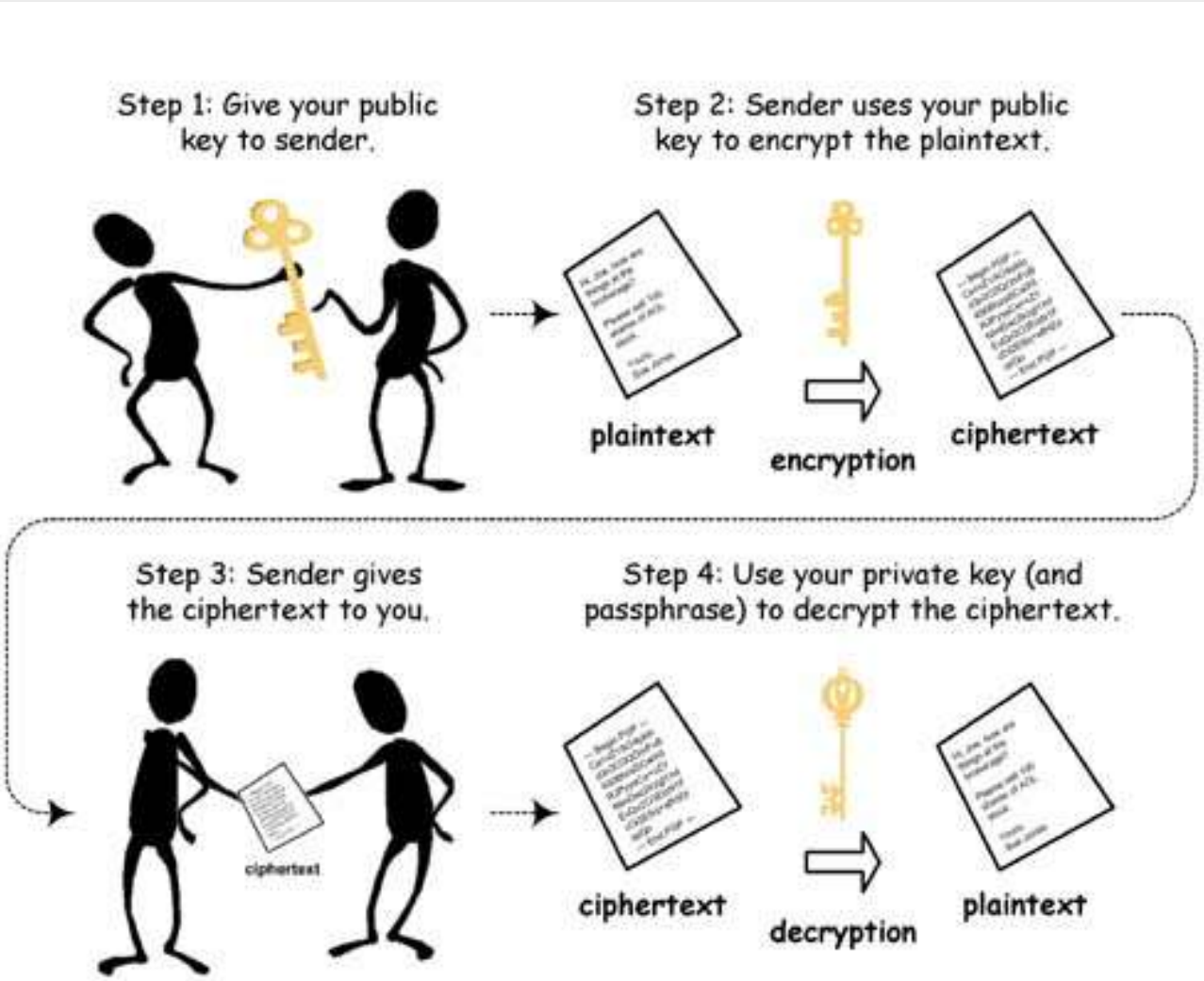
البنية التحتية للمفاتيح العامة
تجيب عن الأسئلة التالية...

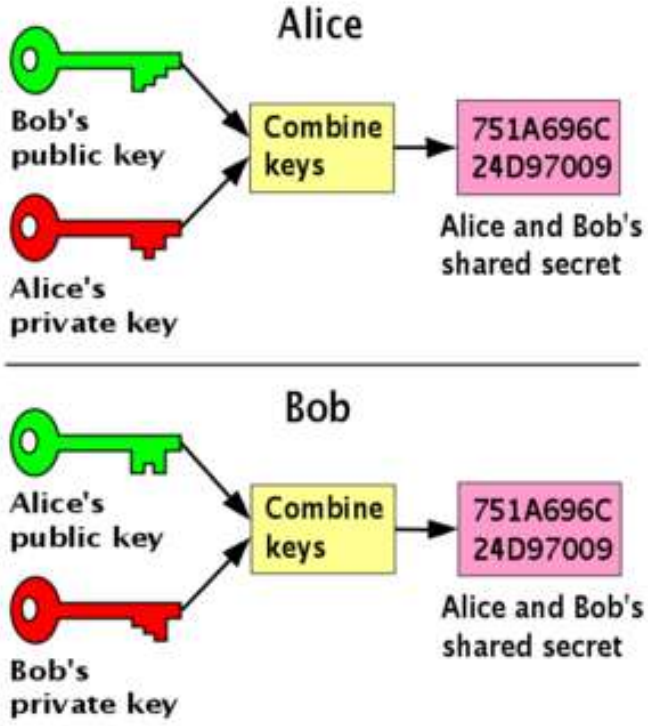
- كيف يستطيع من يستقبل رسالة إلكترونية التأكد من شخصية المرسل؟
- كيف يستطيع المصرف الإلكتروني التأكد من هوية الزبون؟
- كيف لإدارة المرور التأكد من هوية طالب تجديد رخصة القيادة؟
- كيف للمدرسة أو الجامعة التأكد من هوية الطالب الراغب في الإطلاع على سجلاته الدراسية؟
- كيف يتأكد الشخص بأن الموقع هو بالفعل لإدارة المرور أو الجامعة أو المصرف؟
- كيف يستطيع وسيط الأسهم أو المصرف منع الزبون إنكار القيام بعملية ما؟
- كيف يمكن لطرفين التوقيع على عقد تجاري فيما بينهما عن طريق الإنترنت؟
- كيف يمكن إثبات إستلام المرسل إليه للرسالة؟
- كيف للمرسَل إليه إثبات قيام المرسل بإرسال الرسالة؟

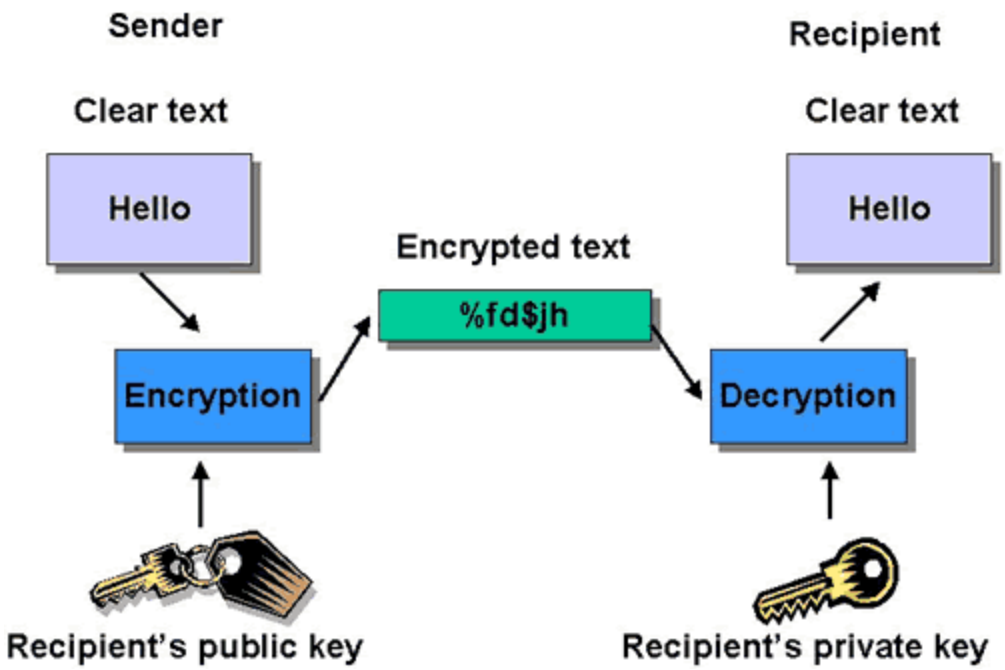
البنية التحتية للمفاتيح العامة
أحد ركائز منظومة التعامل الإلكتروني

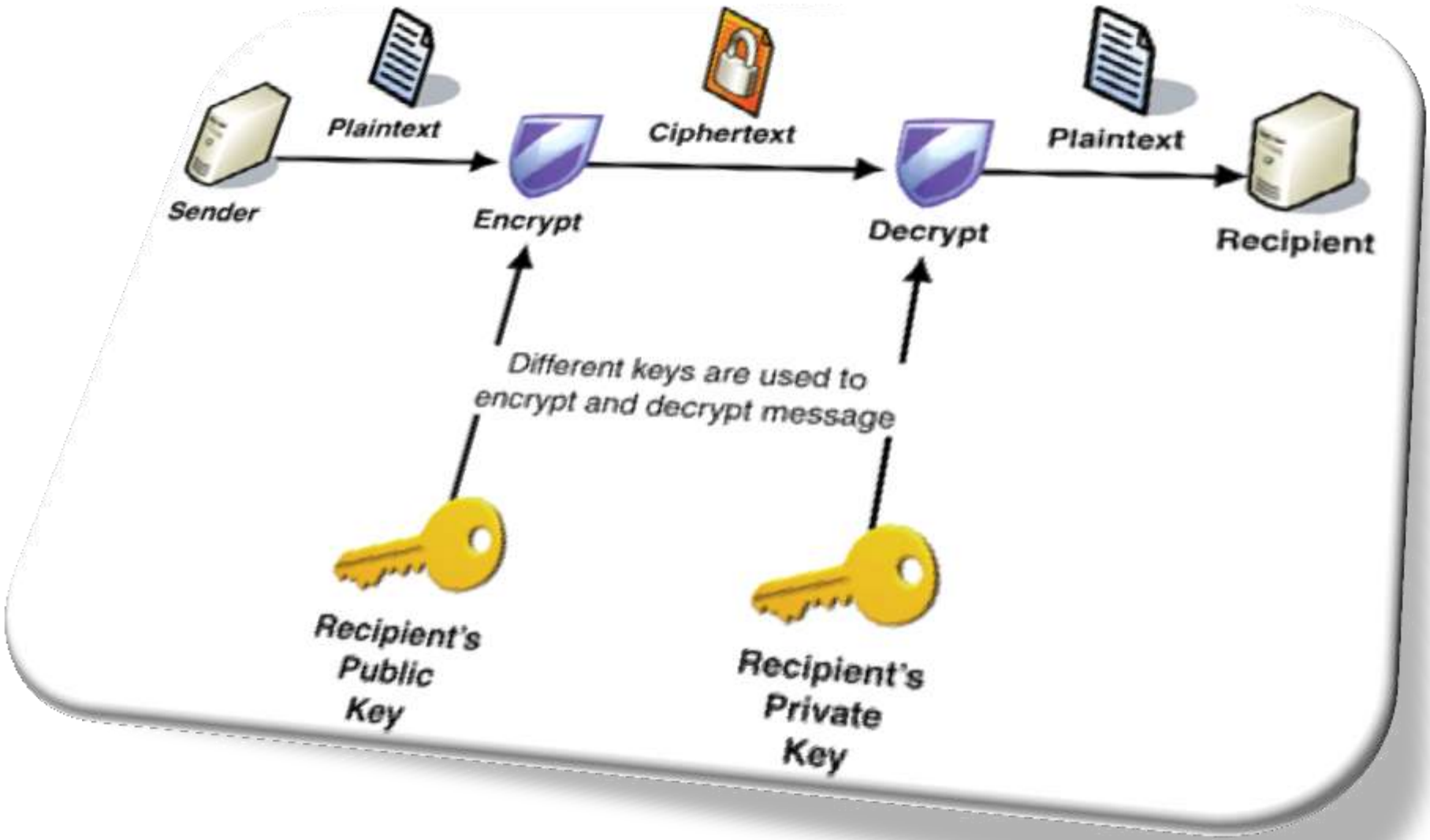
- لكي نتمكن من مزاولة الأعمال الإلكترونية (حكومة إلكترونية، تجارة إلكترونية، تعليم عن بعد، الطب الاتصالي، وغيرها) فنحن بحاجة إلى توفير أربع بنى تحتية هامة، وهي:

  - **المكان:** (البنية التحتية للاتصالات) خطوط الاتصال وشبكات المعلومات ومقدمي خدمة الإنترنت وغيرهم
  - **البيئة الآمنة:** (البنية التحتية للمفاتيح العامة) تعتمد على تقنية التشفير، وتقوم بها مدينة الملك عبد العزيز للعلوم والتقنية ومراكز التصديق
  - **التبادل المالي:** (نظم المدفوعات الإلكترونية) يتم عن طريق نظم المدفوعات وتقوم به مؤسسة النقد العربي السعودي
  - **الأنظمة والقوانين:** (البنية النظامية المتكاملة) لحفظ حقوق المتعاملين وإرساء قواعد التعامل السليم، ويتم عن طريق اللجنة الدائمة للتعامل الإلكتروني بالتعاون مع الجهات التشريعية

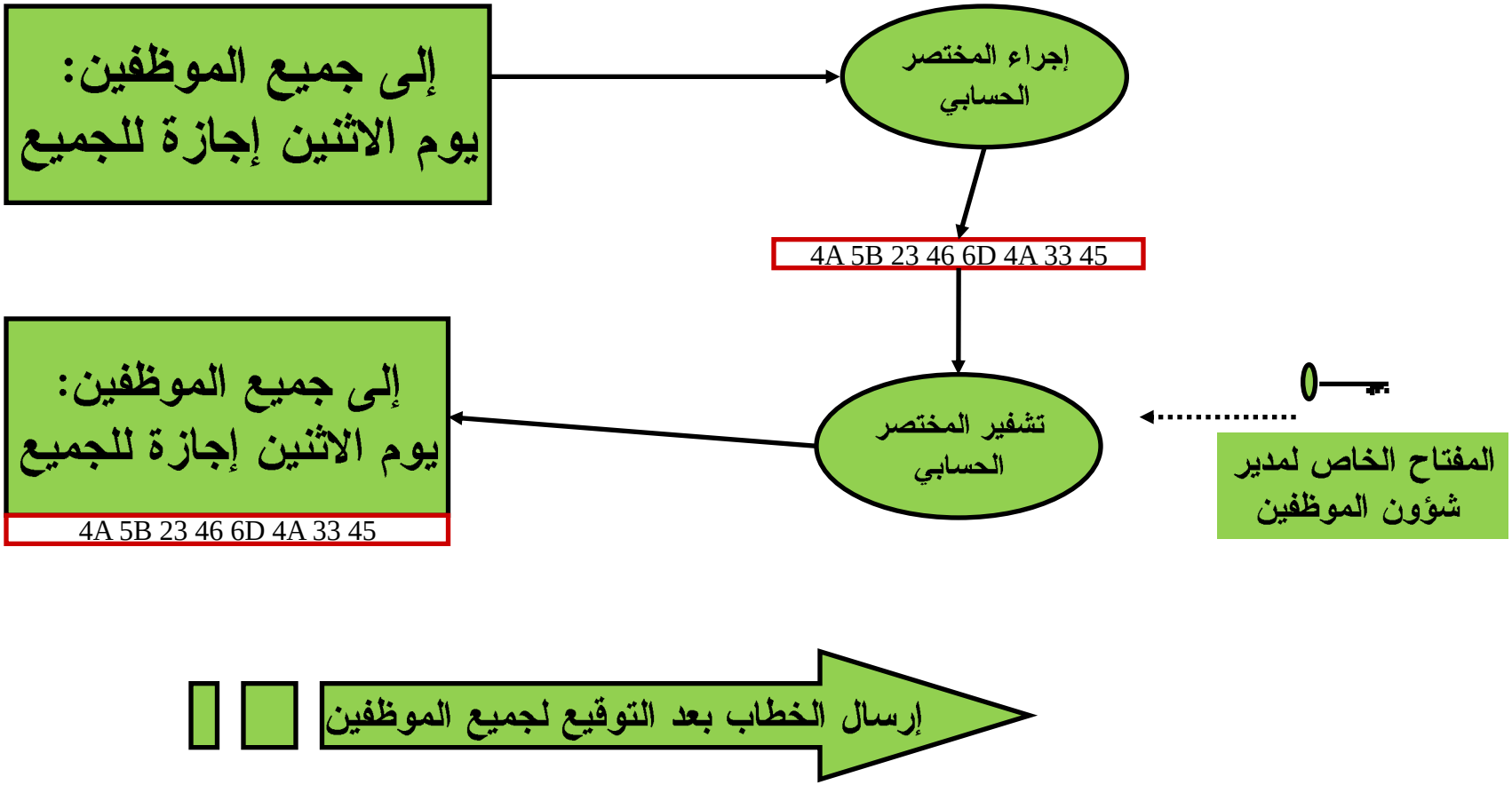

Step 1: Give your public key to sender.
Step 2: Sender uses your public key to encrypt the plaintext.
plaintext
encryption
ciphertext
Step 3: Sender gives the ciphertext to you.
Step 4: Use your private key (and passphrase) to decrypt the ciphertext.
ciphertext
ciphertext
decryption
plaintext


Alice
Bob's public key
Alice's private key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret
Bob
Alice's public key
Bob's private key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret

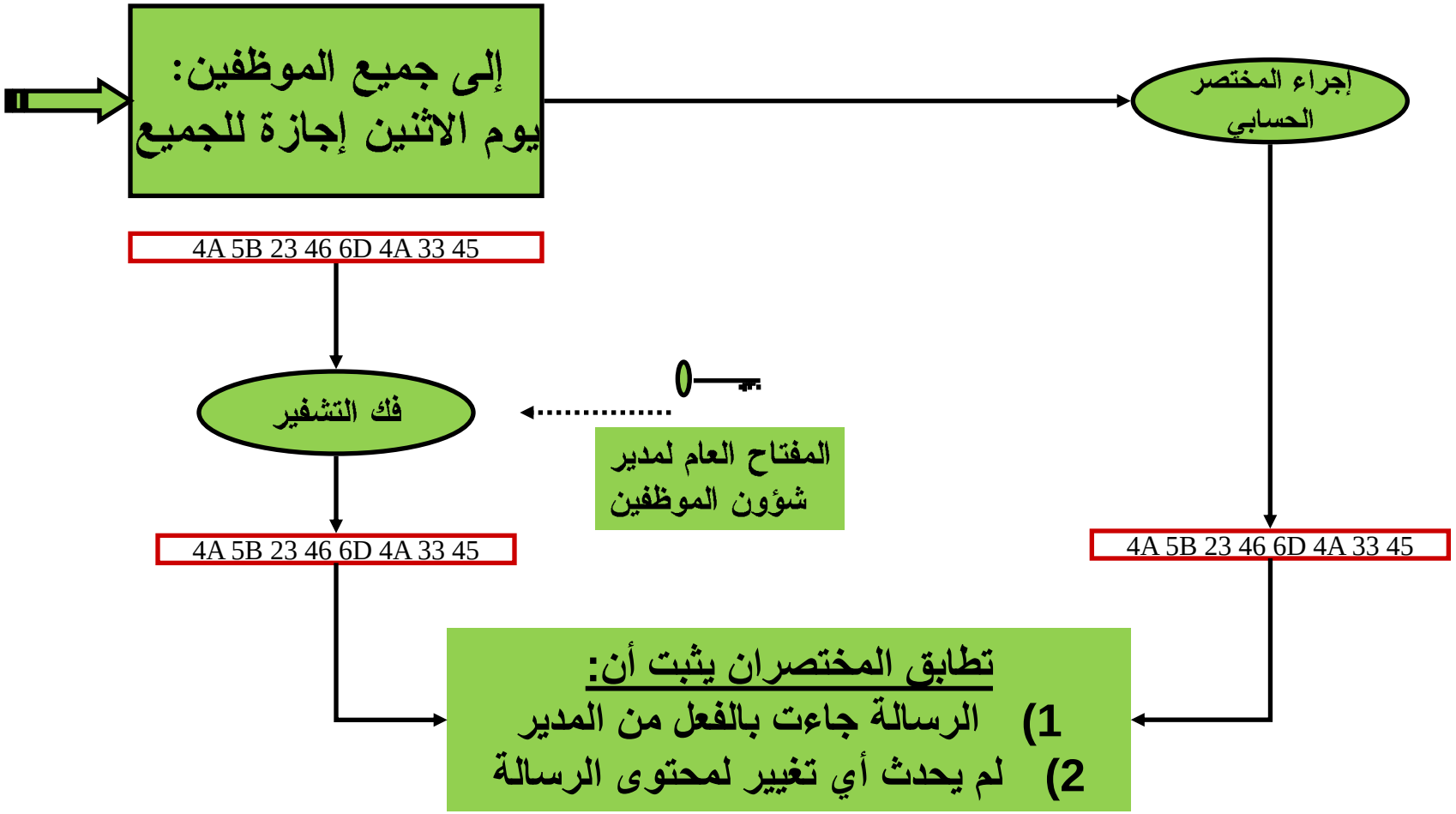

Sender
Clear text
Hello
Encryption
Recipient's public key
Encrypted text
%fd$jh
Recipient
Clear text
Hello
Decryption
Recipient's private key


Plaintext
Ciphertext
Plaintext
Sender
Encrypt
Decrypt
Recipient
Different keys are used to encrypt and decrypt message
Recipient's Public Key
Recipient's Private Key

التوقيع الإلكتروني



التحقق من التوقيع



الحركات المالية الآمنة

- طورت مجموعة من الشركات العالمية بروتوكولا لعمليات الدفع أطلقت عليه بروتوكول الحركات المالية الآمنة بهدف الحفاظ على أمن البيانات وخصوصيتها وسلامتها والتحقق من وصولها إلى الجهة المطلوبة
- التاجر لا يرى رقم البطاقة الائتمانية أثناء الحركات المالية ولكن ترسل الصيغة المشفرة لهذا الرقم إلى مصدر هذه البطاقة للموافقة على إجراء الحركة المالية مع التاجر وتمنع أي تعديل غير مرخص به أثناء إرسال البيانات

نظام التعاملات الإلكترونية

- **يتوفر نظام التعاملات الإلكترونية حالياً بشكل مشروع نظام، ومن المتوقع أن يصدر في أوائل عام 1427 هـ. ويهدف هذا النظام إلى ضبط التعاملات الإلكترونية وتنظيمها وتوفير إطار نظامي لها بما يحقق الأهداف التالية:**
  - **وضع القواعد النظامية لاستخدام التقنية في التعاملات والتوقيعات الإلكترونية، ولتعزيز الثقة بها، وتسهيل استخدامها في القطاعين العام والخاص، بوساطة سجلات إلكترونية يعول عليها.**
  - **تعزيز استخدام التعاملات الإلكترونية على الصعيدين المحلي والدولي، للاستفادة منها في جميع المجالات، كالتجارة، والطب، والتعليم، والحكومة الإلكترونية، والدفع الإلكتروني، وإلى غير ذلك من التطبيقات.**
  - **إزالة أي عائق أمام استخدام التعاملات والتوقيعات الإلكترونية.**
  - **الحد من حالات إساءة الاستخدام و فرص الاحتيال في التعاملات والتوقيعات الإلكترونية، كالتزوير والاختلاس.**

الأنظمة الرقمية