جامعة القدس المفتوحة

كلية تكنولوجيا المعلومات والعلوم التطبيقية

قسم امن المعلومات

الملحق العملي

مقرر: مبادئ علم التشفير

رقم المقرر: 1374

اعداد: دكتور امجد محفوظ

فرع طولكرم

ملخص Abstract :

يهدف هذا الملحق الى وصف وشرح طبيعة الجانب العملي لمقرر مبادئ علم التشفير و رقمه 1374 من اجل الامتحان العملي فيما بتعلق ب عضو هيئة التدريس والطالب.

الاهداف:

يهدف هذا الملحق الى ما يلي:

1. التعريف بمصطلحات ومفاهيم واساليب التشفير
2. معرفة انواع التشفير المستخدمة حاليا لحماية المعلومات.
3. معرفة مفهوم التشفير لتدفق البيانات Stream Cipher.
4. معرفة مفهوم التشفير الكتلي Block Cipher.
5. التعرف على اسلوب التشفير المتناظر Symmetric – Key Encipherment
6. اسلوب التشفير غير المتناظرAsymmetric – Key Encipherment
7. الجانب العملي المطلوب

المحتويات:

اولا: التشفير :

- بشكل عام هو الاداة الاساسية لامن المعلومات، ويعتمد على اسلوب علم الرياضيات في عملية التشفير وفك التشفير. ويستخدم في عدة مجالات منها تخزين المعلومات او نقل المعلومات من مكان الى مكان او نقلها عبر الشبكات لضمان عدم الوصول اليها او قراءتها من الاشخاص غير المصرح لهم .
- و يعرف التشفير على انه اخفاء المعطيات (المعلومات) للحفاظ على سريتها. وهو يتضمن تحويل النص من صيغة مفهومه ومقروءة وتسمى في هذه الحالة ب النص الواضح Plain text او الرسائل Messages الى صيغة اخرى غير مفهومة وغير واضحة وتسمى في هذه الحالة Cipher text او النص المشفر.

ثانيا: اهداف التشفير:

في هذا القسم سنتعرف على اهداف التشفير والفائدة المرجوة من استخدام التشفير:

1. ضمان اخصوصية.
2. تكامل البيانات.
3. الموثوقية.
4. عدم الانكار.
5. التحكم في الوصول.

ثالثا: مكونات خوارزمية التشفير:

1. النص الواضح وهو النص الصريح ويسمى Plain text ويرمز له بالرمز (P) او(M) تسمى بالمعطيات او المعلومات و تكون بصيغة مفهومة ومقروءة وتستخدم لاتخاذ القرار منها وتتمثل في المدخلات اوالمخرجات والتي تقودنا الى المعرفة وتحديد القرارات في المؤسسة وهي البيانات الاصلية التي يتم ادخالها في خوارزمية التشفير.

2. النص المشفر ويسمى Cipher text وهو نص غير صريح بمعنى انه غير واضح ولا يمكن قراءاته او التعرف على معنى الكلمات ولا يفيد في اتخاذ اي قرار او دلالات اخرى وهي بيانات مخرجة بعد عملية التشفير وتعتمد على المفتاح السري و النص الواضح.

3. المفاتيح : وتسمى ال Keys وهو المفتاح المستخدم في عملية التشفير وفك التشفير. اما ان يكون مفتاح واحد او اكثر من مفتاح وذلك حسب طبيعة الخوارزمية المستخدمة.

4. خورازمية التشفير Encryption Algorithm وهي الخوارزمية المستخدمة في اسلوب تشفير النص لتحويله من نص واضح الى نص غير واضح مستعينا ب المفاتيح المستخدمة فيه، وتحتوي على بدائل وتحولات مختلفة على التص الواضح.

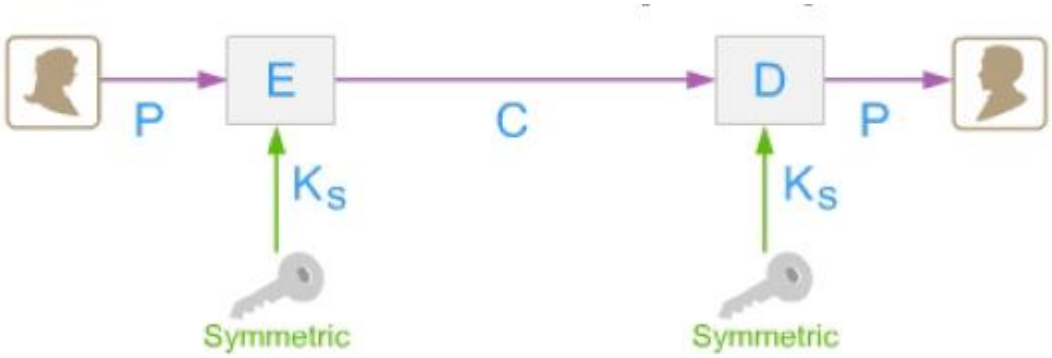
5. خوارزمية فك التشفير Decryption Algorithm وهي الخوارزمية المستخدمة في فك التشفير وتاخذ النص المشفر والمفتاح السري وتقوم بانتاج النص الواضح وهو النص الصريح.

رابعا: انواع التشفير:

يقسم التشفير من حيث الاسلوب والتقنيات الى:

1. التشفير بمفتاح متناظر Symmetric Key Encipherment

وفق هذه التقنية يجري الشفير باستخدام مفتاح سري مشترك بين المرسل والمستقبل ويسمى Shared Private Keys وهو يستخدم نفس المفتاح في عمل التشفير وفك التشفير للنص. الشكل التالي يوضح هذا الاسلوب.

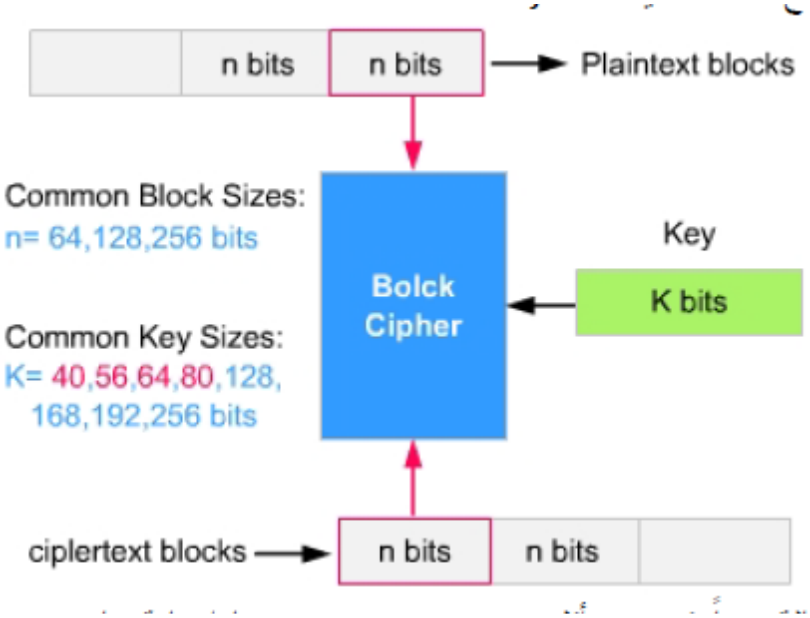


تقسم الخوارزميات التناظرية الى صنفين و هما:

ا. خوارزميات التدفق (مشفرات التدفق): تسمى ب Stream Cipher وهي خوارزميات تعمل على النص الواضح كثنائية واحدة bit by bit او على مستوى البايب byte في الوقت الواحد. ويكون لدينا في هذه الحالة دفق stream لمعطيات النص غير المشفر(النص الواضح) ودفق اخر لمعطيات النص المشفر كما هو موضح في الشكل التالي:

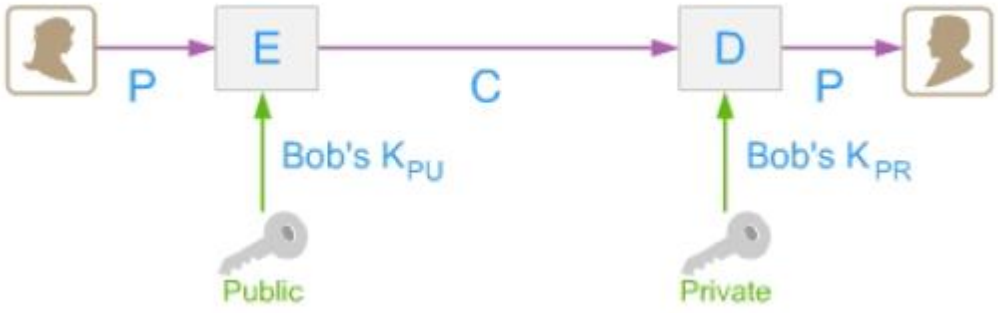
$$P = P_1 P_2 P_3 \cdots$$
$$C = C_1 C_2 C_3 \cdots$$
$$K = (k_1, k_2, k_3, \cdots)$$
$$C_1 = E_{k1}(P_1)$$
$$C_2 = E_{k2}(P_2)$$
$$C_3 = E_{k3}(P_3) \cdots$$

ب. خوارزميات الكتل (المشفرات الكتلية) : وتسمى Block Cipher وهي خوارزميات تعمل على النص الواضح بشكل كتل (مجاميع من الثنائيات) وتستخدم لعمل تشفير ل قواعد بيانات ضخمة من خلال تقسيم النص غير المشفر الى كتل بحجم متساوي (حجم n) ليتم بعدها تشفيرها معا وانشاء كتلة من نفس حجم النص المشفر كما هو موضح في الشكل التالي.



2. التشفير بمفتاح غير متناظر Asymmetric Key Encipherment

وفق هذه التقنية يجري الشفير باستخدام مفتاحين احدهما معلن للجميع ويسمى المفتاح العام Public key والمفتاح الاخر يسمى المفتاح الخاص(السري) Private key. لعمل تشفير بين طرفين فان النص الواضح يشفر باستخدام المفتاح العام ل الطرف المستقبل والذي يقوم بدوره (الطرف المستقبل) بفك النص المشفر من خلال المفتاح الخاص الذي يملكه، مع العلم بانه لا يمكن لاي طرف فك التشفير لان النص قد شفر بالاصل من خلال المفتاح العام المرتبط به. الشكل التالي يوضح الية عمل هذا الاسلوب من التشفير.



خامسا: الجانب العملي المقترح (المشروع العملي):

المطلوب في الامتحان العملي هو كالاتي:

- يقوم الطالب بعمل تشفير وفك التشفير باستخدام احدى الطرق التالية المقترحه حسب ما يراه عضو هيئة التدريس :
  1. لغات البرمجة التي تعلمها سابقا.
  2. استخدام برامج اخرى مثل اكسل وذلك من خلال انشاء ملف تطبيقي يحتوي على حقل النص الواضح و حقل النص المشفر وحقل المفتاح ويقوم التطبيق بعمل التشفير وفك التشفير بناء على خوارزميات التشفير مستعينا ب المقاطع البرمجية مثل VB script, macro, developer وكتابة المقاطع البرمجية لحوسبة وبناء التطبيق.
  3. برنامج ماتلاب Mat Lap واستخدام الادوات المتوفره فيه وكتابة المقاطع البرمجية والاكواد لعمل التشفير وفك التشفير.
  4. اي برنامج اخر يقترحه عضو هيئة التدريس بما يتناسب مع طبيعة المقرر.

- المشروع العملي المقدم من الطالب يتضمن البرنامجين الاتين ويرصد له 70 علامه:
  1. البرنامج الاول لعمل تشفير وفك التشفير باستخدام خوارزميات المفتاح المتناظر.
  2. البرنامج الثاني لعمل تشفير وفك تشفير باستخدام خوارزميات المفتاح غير المتناظر.
  3. كتابة تقرير من قبل الطالب عن البرنامجين بحيث يتضمن وصف التطبيق وطريقة التشفير المستخدمة والمدخلات والمخرجات وطريقة فك التشفير و وصف الاكواد المستخدمة في التطبيق ويرصد له 30 علامه.

- يتم تطبيقه امام عضو هيئة التدريس وتنفيذه في المختبر ومناقشة الطالب عن مشروعه والتاكد من صحة عمل الخوارزمية المستخدمة في البرنامج.

- اختبار البرامج من خلال ادخال نص معين او القراءة من ملف لعمل التشفير او من قاعدة بيانات.

- التاكد من ان الطالب قام هو بنفسه في كتابة الاكواد البرمجية وليس منسوخ من الانترنت او من عمل طالب اخر.

- عضو هيئة التدريس له الخيار في عملية تقييم الطالب بما يراه مناسبا مع الالتزام في المتطلبات الاساسية للمشروع.

- يمكن لعضو هيئة التدريس اقتراح طريقة معينه لنوع الخوارزمية المطلوبة لعمل التشفير و فك التشفير بما يراه مناسبا .

النهاية...