جامعة المنارة
كلية الهندسة
معلوماتية

جلسة العملي الرابعة
Information System Security
أمن نظم المعلومات

مدرسة المقرر
د. بشرى علي معلا

المسألة الأولى

من أجل خوارزمية ديفي هيلمان لتبادل المفاتيح، بفرض لدينا العددين الأوليين 7 ,23 المطلوب:

وضح خطوات وقيم توليد المفتاح السري (المتناظر) بين الطرفين أليس و بوب . علماً أن القيم العشوائية التي يختارها الطرفان هي 3و6

حل المسألة الأولى

أليس | **بوب**

الاتفاق على قيم g=7,P=23

تختار عدداً عشوائياً: XA=6

يختار عدداً عشوائياً XB=3

تولد قيمة عامة YA وفق العلاقة :

$$YA = g^{XA} mod\ P$$

$$YA = 7^{6} mod\ 23 = 4$$

يولد قيمة عامة YB وفق العلاقة :

$$YB = g^{XB} mod\ P$$

$$YB = 7^{3} mod\ 23 = 21$$

تولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = (YB)^{XA} mod\ P = (21)^{6} mod\ 23 = 18$$

يولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = (YA)^{XB} mod\ P = (4)^{3} mod\ 23 = 18$$

المسألة الثانية

من أجل خوارزمية ديفي هيلمان لتبادل المفاتيح، بفرض لدينا العددين الأوليين 5 و 23 المطلوب:

1. وضح خطوات وقيم توليد المفتاح السري (المتناظر) بين الطرفين أليس و بوب .علماً أن القيم العشوائية التي يختارها الطرفان هي 3و4 .

2 . ما هي القيم التي يمكن للمهاجم أن يحصل عليها عند تطبيق خوارزمية ديفي هيلمان السابقة ؟ علل إجابتك

حل المسألة الثانية

الطلب الأول:

الاتفاق على قيم g=5,P=23

أليس

تختار عدداً عشوائياً XA=4

تولد قيمة عامة YA وفق العلاقة :

$$YA = g^{XA} mod\ P$$
$$YA = 5^4 mod\ 23 = 4$$

بوب

يختار عدداً عشوائياً XB=3

يولد قيمة عامة YB وفق العلاقة :

$$YB = g^{XB} mod\ P$$
$$YB = 5^3 mod\ 23 = 10$$

تولد المفتاح السري (المتناظر) وفق العلاقة:

$$\mathrm{K} = (YB)^{XA} mod\ P = (10)^4 mod\ 23 = 18$$

يولد المفتاح السري (المتناظر) وفق العلاقة:

$$\mathrm{K} = (YA)^{XB} mod\ P = (4)^3 mod\ 23 = 18$$

حل المسألة الثانية

الطلب الثاني:

القيم التي يمكن يحصل عليها المهاجم:

g=5,P=23 لأنها قيم عامة متفق عليها

YA=4,YB=10 لأنها قيم عامة متبادلة

المسألة الثالثة

من أجل خوارزمية ديفي هيلمان لتبادل المفاتيح، بفرض لدينا العددين الأوليين 7 و 17 المطلوب:

وضح خطوات وقيم توليد المفتاح السري (المتناظر) بين الطرفين أليس و بوب .علماً أن القيم العشوائية التي يختارها الطرفان هي 3و2 .

حل المسألة الثالثة

الطلب الأول:

الاتفاق على قيم g=7,P=17

أليس

تختار عدداً عشوائياً XA=2

تولد قيمة عامة YA وفق العلاقة :

$$YA = g^{XA} mod\ P$$
$$YA = 7^2 mod\ 17 = 15$$

بوب

يختار عدداً عشوائياً XB=3

يولد قيمة عامة YB وفق العلاقة :

$$YB = g^{XB} mod\ P$$
$$YB = 7^3 mod\ 17 = 3$$

تولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = (YB)^{XA} mod\ P = (3)^2 mod\ 17 = 9$$

يولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = (YA)^{XB} mod\ P = (15)^3 mod\ 17 = 9$$

جَامعة
المَنارة
MANARA UNIVERSITY

نهاية الجلسة