

جلسة العملي الخامسة  
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 23,7 المطلوب:  
وضح خطوات وقيم توليد المفتاح السري (المتناظر) بين الطرفين أليس و بوب . علماً أن القيم العشوائية  
التي يختارها الطرفان هي 3 و6

بوب

الاتفاق على قيم  $g=7, P=23$

أليس

يختار عدداً عشوائياً  $X_B=3$

يولد قيمة عامة  $Y_B$  وفق العلاقة:

$$Y_B = g^{X_B} \text{ mod } P$$

$$Y_B = 7^3 \text{ mod } 23 = 21$$

يولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = (Y_A)^{X_B} \text{ mod } P = (4)^3 \text{ mod } 23 = 18$$

تختار عدداً عشوائياً:  $X_A=6$

تولد قيمة عامة  $Y_A$  وفق العلاقة:

$$Y_A = g^{X_A} \text{ mod } P$$

$$Y_A = 7^6 \text{ mod } 23 = 4$$

تولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = (Y_B)^{X_A} \text{ mod } P = (21)^6 \text{ mod } 23 = 18$$

## 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 3 و 4.

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

الاتفاق على قيم  $g=5, P=23$

بوب

يختار عدداً عشوائياً  $X_B=3$

يولد قيمة عامة  $Y_B$  وفق العلاقة:

$$Y_B = g^{X_B} \text{ mod } P$$
$$Y_B = 5^3 \text{ mod } 23 = 10$$

يولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = (Y_A)^{X_B} \text{ mod } P = (4)^3 \text{ mod } 23 = 18$$

أليس

تختار عدداً عشوائياً  $X_A=4$

تولد قيمة عامة  $Y_A$  وفق العلاقة:

$$Y_A = g^{X_A} \text{ mod } P$$
$$Y_A = 5^4 \text{ mod } 23 = 4$$

تولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = (Y_B)^{X_A} \text{ mod } P = (10)^4 \text{ mod } 23 = 18$$

## 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 3 و 2.

الاتفاق على قيم  $g=7, P=17$

بوب

يختار عدداً عشوائياً  $X_B=3$

يولد قيمة عامة  $Y_B$  وفق العلاقة:

$$Y_B = g^{X_B} \bmod P$$
$$Y_B = 7^3 \bmod 17 = 3$$

يولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = (Y_A)^{X_B} \bmod P = (15)^3 \bmod 17 = 9$$

أليس

تختار عدداً عشوائياً  $X_A=2$

تولد قيمة عامة  $Y_A$  وفق العلاقة:

$$Y_A = g^{X_A} \bmod P$$
$$Y_A = 7^2 \bmod 17 = 15$$

تولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = (Y_B)^{X_A} \bmod P = (3)^2 \bmod 17 = 9$$

# نهاية الجلسة