

أمن نظم المعلومات

مدرسة المقرر

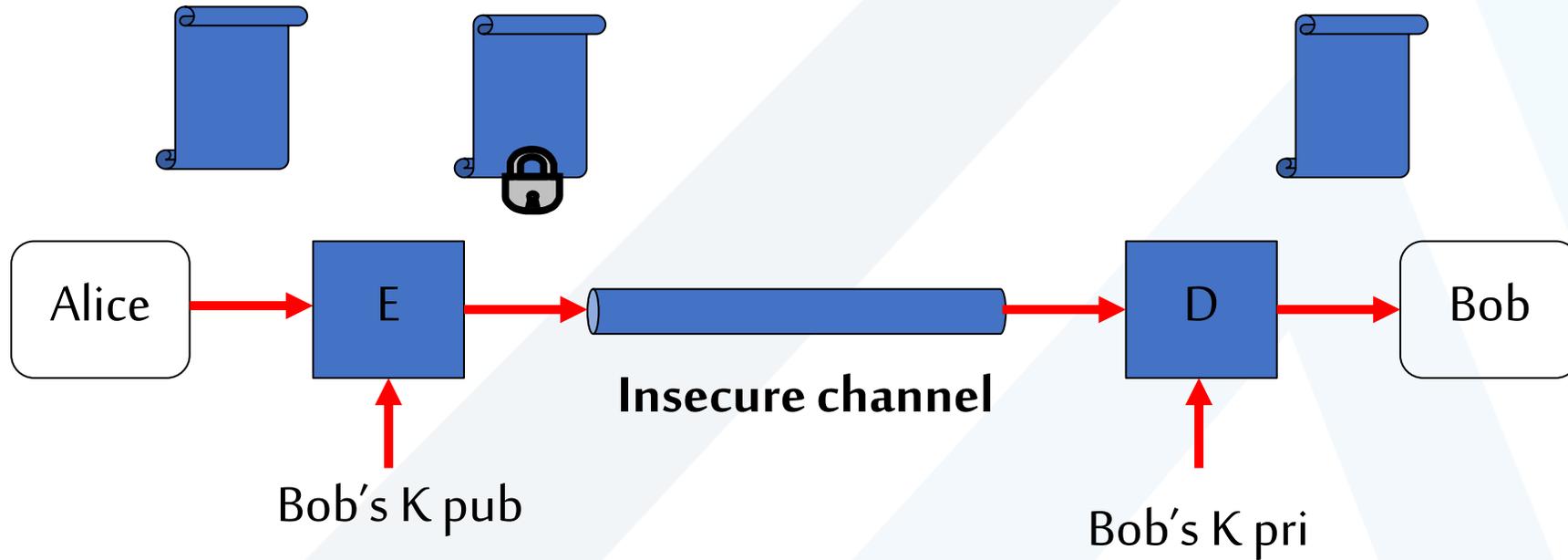
د. بشرى علي معلا

عناوين المحاضرة الثالثة

- تذكرة بمفهوم التشفير غير المتناظر
- مفهوم التابع وحيد الاتجاه (one-way function)
- مفهوم تابع ال mod
- نظام تشفير حقيبة الظهر (knapsack Cryptosystem)

تذكرة بمفهوم التشفير غير المتناظر

يعتمد التشفير غير المتناظر على استخدام مفتاحين: مفتاح خاص private key و مفتاح عام public key



يشفر باستخدام المفتاح العام للمستقبل و يفك التشفير باستخدام المفتاح الخاص المقابل (للمستقبل نفسه)

مفهوم التابع وحيد الاتجاه (one way function)

❖ نقول عن تابع $y=f(x)$ أنه تابع وحيد الاتجاه ، إذا تحققت لدينا الشروط الآتية:

✓ إذا توفر لدينا x فإنه من السهل حساب $y=f(x)$

✓ أما إذا توفر لدينا y فإنه لا يمكن حسابياً تحديد قيمة $x: x = f^{-1}(y)$

❖ مثال : تابع حساب العوامل الأولية

إذا كان لدينا العددين الأوليين الكبيرين p, q من السهل جداً حساب $n=p \times q$

لكن عند معرفة n من غير الممكن معرفة العددين الأوليين اللذين ينتج عنهما n بل يجب تجربة كافة القيم .

❖ قد يعاني تابع وحيد الاتجاه مما يسمى المصيدة

مفهوم التابع وحيد الاتجاه (one way function)

❖ مثال على المصيدة :

في حساب العددين الأوليين تعد معرفة أحدهما هي مصيدة تتسبب بمعرفة الآخر فمثلاً بمعرفة n مع معرفة q سيكون من السهل معرفة p أي أن q هي مصيدة لحساب p من n

مفهوم تابع ال mod (1/3)

➤ يعرف تابع ال mod بالعلاقة: $a = b \text{ mod}(n)$

و تعني أن a هو باقي قسمة b على n .

➤ إن الأعداد التي تؤخذ بالحسبان هي فقط الأعداد الصحيحة غير السالبة من المعاملات (modulus) .

➤ من أجل mod(n) تكون الأعداد الفعالة هي فقط الأعداد من 0 إلى (n-1) . ونتائج العمليات ستكون دائماً من 0 حتى (n-1)

مثال:

$$1 = 11 \text{ mod } 5$$

تعني أن باقي قسمة 11 على 5 هو 1

$$4 = 73 \text{ mod } 23$$

تعني أن باقي قسمة 73 على 23 هو 4

مفهوم تابع الـ mod (2/3)

❖ الأعداد المتطابقة في القياس:

✓ نقول عن عددين أنهما عددين متطابقين في القياس إذا كان:

$$(a \bmod(n)) = (b \bmod(n))$$

✓ و يعبر عن ذلك رياضياً كمايلي : $a \equiv b \bmod(n)$

$$\left. \begin{array}{l} 11 \bmod 5 = 1 \\ 1 \bmod 5 = 1 \end{array} \right\} \Rightarrow 11 \equiv 1 \bmod(5) \quad \text{مثال:}$$

$$\left. \begin{array}{l} 73 \bmod 23 = 4 \\ 4 \bmod 23 = 4 \end{array} \right\} \Rightarrow 73 \equiv 4 \bmod(23)$$

❖ عمليات الحساب بالقياس: $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$



جامعة
المنارة
MANARA UNIVERSITY

مفهوم تابع ال mod (3/3)

❖ معكوس الضرب بالنسبة لتابع ال mod :

✓ معكوس عدد a بالنسبة لتابع $\text{mod}(m)$ هو عدد x بحيث $a * x \equiv 1 \text{mod}(m)$

تكون قيمة x ضمن المجال $\{0,1,2,\dots,m-1\}$

مثال :

$$8 * x \equiv 1 \text{mod}(29)$$

أوجد معكوس العدد 8 للضرب بالنسبة لـ $\text{mod}(29)$

$$88 = 1 \text{mod}(29)$$

تكون قيمة x ضمن المجال $\{0,1,2,3,4,5,6,7,8,\dots,28\}$

$$8 * 11 \equiv 1 \text{mod}(29)$$

$$88 = 8 * 11$$

أي $x=11$ هي معكوس الضرب لـ $a=8$ بالنسبة لـ $\text{mod}29$

نظام تشفير حقيبة الظهر (1/2) knapsack Cryptosystem

❖ يعد أول نظام تشفير غير متناظر ، وضع من قبل العالمين Hellman و Merkel عام 1978 ، يمكن تنظيم هذا النظام كالآتي:

➤ **الفكرة الرئيسية:**

إيجاد حل لمسألة تعبئة حقيبة الظهر

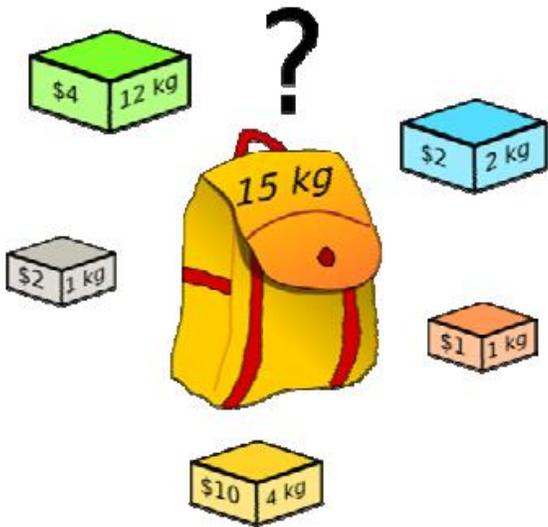
➤ **فرضيات المسألة:**

حقيبة سعتهما S

عدد الأغراض K غرض

➤ **المطلوب:**

ما هي مجموعة الأغراض التي يجب اختيارها كي تمتلئ الحقيبة تماماً؟



نظام تشفير حقيبة الظهر (2/2) knapsack Cryptosystem

❖ التوصيف الرياضي للمسألة:

$$S = X_1 a_1 + X_2 a_2 + \dots + X_k a_k$$

حجم الحقيبة:

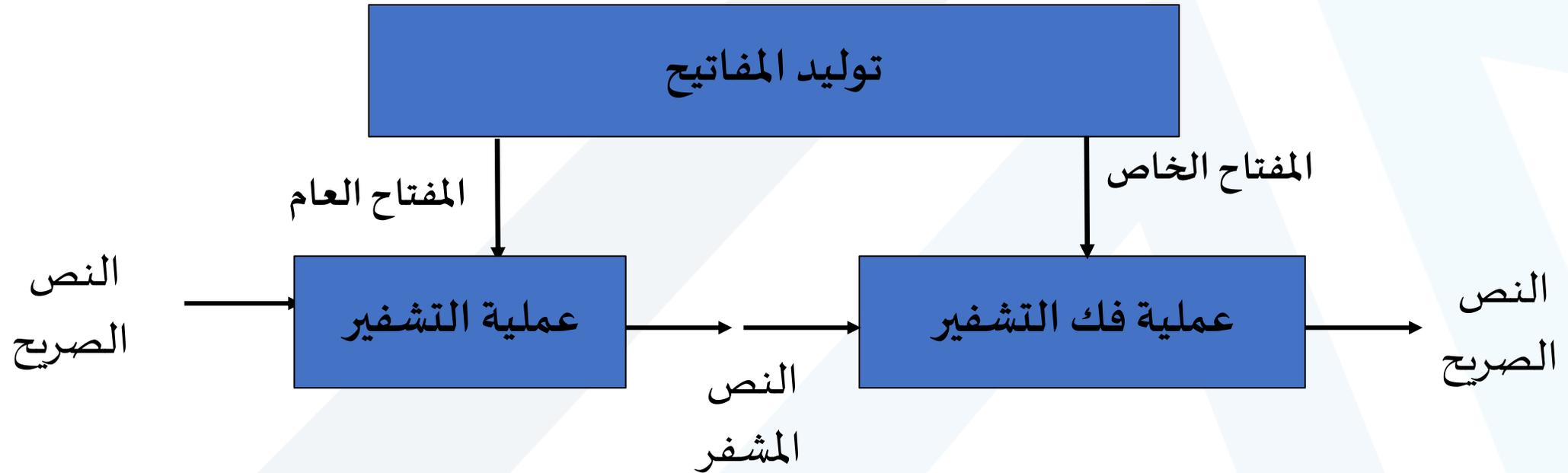
■ حيث:

a_i حجم الغرض i

X_i قيمتها 0 أو 1 حيث: $X_i = 0$, الغرض i غير موجود ضمن الحقيبة

$X_i = 1$ الغرض i موجود ضمن الحقيبة

المخطط الصندوقي لنظام تشفير حقيبة الظهر knapsack Cryptosystem





جامعة
المنارة
MANARA UNIVERSITY

مراحل نظام تشفير حقبة الظهر (1/4)

❖ توليد المفاتيح : خطوات توليد المفتاح العام والمفتاح الخاص:

من أجل عدد أغراض K :

1. نقوم بتوليد مجموعة متزايدة $b = [b_1, b_2, \dots, b_k]$ بحيث تحقق الشرط

$$b_i \geq b_1 + b_2 + \dots + b_{i-1}$$

2. نختار قيمة n بحيث تحقق الشرط : $n > b_1 + b_2 + \dots + b_k$

3. نختار قيمة r بحيث تكون أولية مع n

4. نحسب المصفوفة t باستخدام العلاقة : $t_i = (b_i \times r) \bmod(n)$

5. ندور t وفق تدوير مفروض و بذلك نحصل على **المفتاح العام** a

6. و يكون المفتاح الخاص هو **القيم b و n و r والتدوير**

مثال عن توليد المفاتيح في نظام تشفير حقيبة الظهر (1/2)

بفرض عدد الأغراض $K=4$.

1. نقوم بتوليد مجموعة متزايدة $b = [2,3,6,12]$ و هي تحقق الشرط

$$b_i \geq b_1 + b_2 + \dots + b_{i-1}$$

محقق $3 \geq b_1 = 2$

محقق $6 \geq b_1 + b_2 = 2 + 3 = 5$

محقق $12 \geq b_1 + b_2 + b_3 = 2 + 3 + 6 = 11$

2. نختار n بحيث هي تحقق الشرط $n > b_1 + b_2 + b_3 + b_4$

$n=25$ هي تحقق الشرط $n > 2 + 3 + 6 + 12 = 23$

مثال عن توليد المفاتيح في نظام تشفير حقبة الظهر (2/2)

3. نختار قيمة $r=7$ وهي أولية مع $n=25$

4. نحسب بعدها المصفوفة t باستخدام العلاقة: $t_i = (b_i \times r) \bmod(n)$

$$t_1 = (b_1 \times r) \bmod(n) = (2 \times 7) \bmod(25) = 14$$

$$t_2 = (b_2 \times r) \bmod(n) = (3 \times 7) \bmod(25) = 21$$

$$t_3 = (b_3 \times r) \bmod(n) = (6 \times 7) \bmod(25) = 17$$

$$t_4 = (b_4 \times r) \bmod(n) = (12 \times 7) \bmod(25) = 9$$

فتكون المصفوفة $t=[14,21,17,9]$

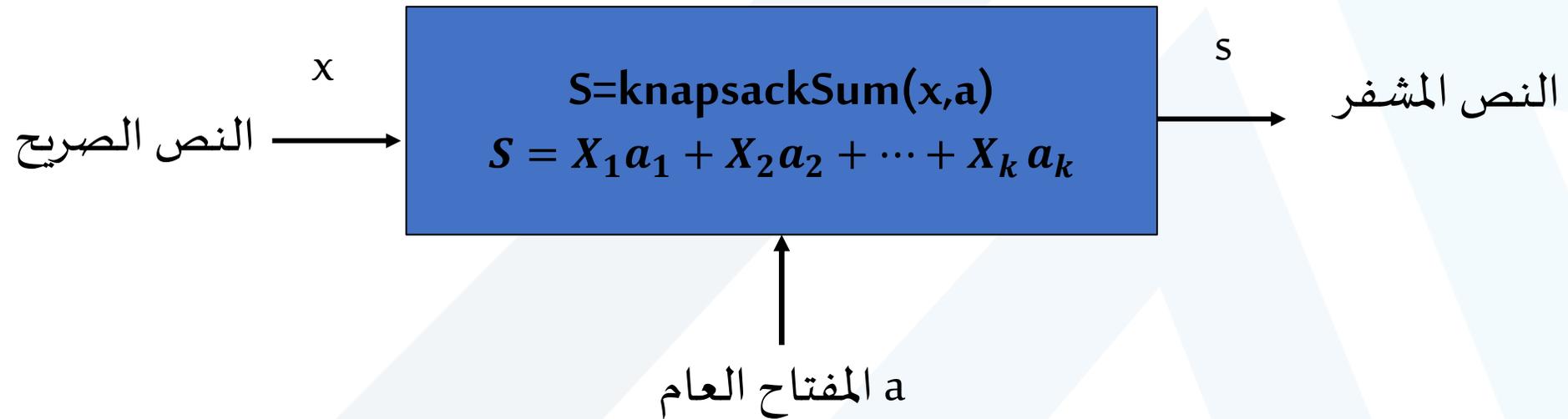
5. بفرض أن التدوير هو: $[3,2,4,1]$

بعد تدوير t ينتج المفتاح العام: $a=[17, 21,9,14]$

ويكون المفاتيح الخاص: $n=25, r=7, b=[2,3,6,12]$ و التدوير: $[3,2,4,1]$

مراحل نظام تشفير حقيبة الظهر (2/4)

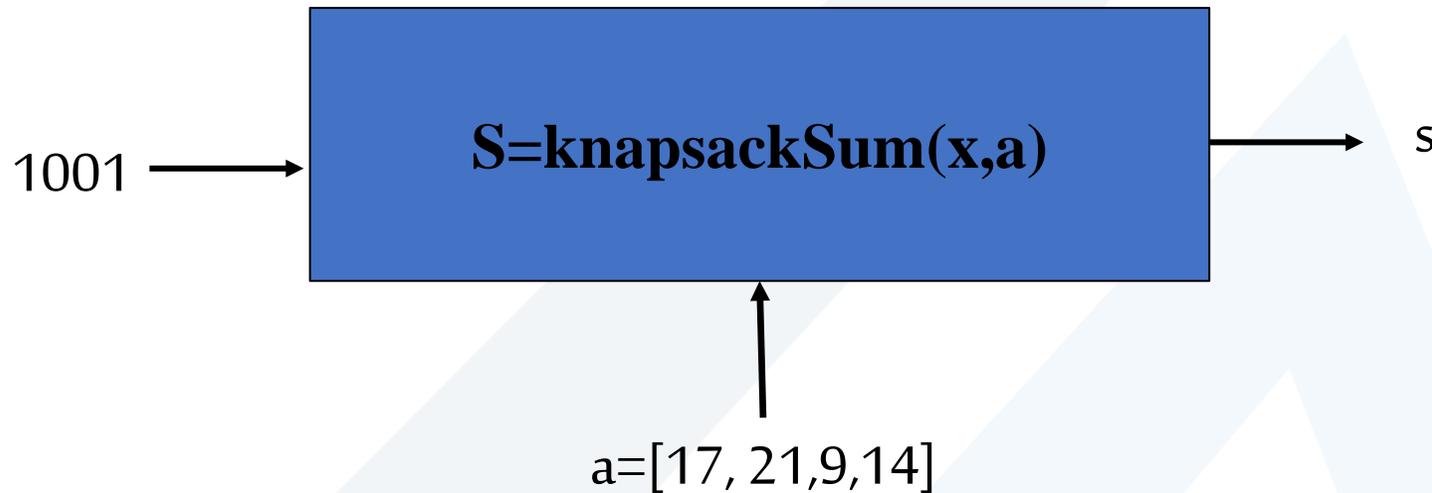
عملية التشفير ❖



المخطط الصندوقي

مثال أعلى عملية التشفير باستخدام حقيبة الظهر

بفرض أن النص الصريح $x=1001$. أوجد النص المشفر باستخدام نظام حقيبة الظهر (s) الذي يعتمد القيم المحسوبة سابقاً



$$S = X_1 a_1 + X_2 a_2 + X_3 a_3 + X_4 a_4$$

$$S = 1 * 17 + 0 * 21 + 0 * 9 + 1 * 14 = 31$$

النص المشفر



جامعة
المنارة
MANARA UNIVERSITY

مثال ٢ على عملية التشفير باستخدام حقبة الظهر

بفرض أن النص الصريح $x=00101101$. أوجد النص المشفر باستخدام نظام حقبة الظهر (s) الذي يعتمد القيم المحسوبة سابقاً

نلاحظ أن طول النص الصريح يساوي 8 وهو أكبر من عدد الأغراض 4

نقسم هذا النص على طول الأغراض فيكون: $x_1=0010$

$x_2=1101$

$a=[17, 21, 9, 14]$

$$S1 = X_1 a_1 + X_2 a_2 + X_3 a_3 + X_4 a_4$$

$$S1 = 0.17 + 0.21 + 1.9 + 0.14 = 9$$

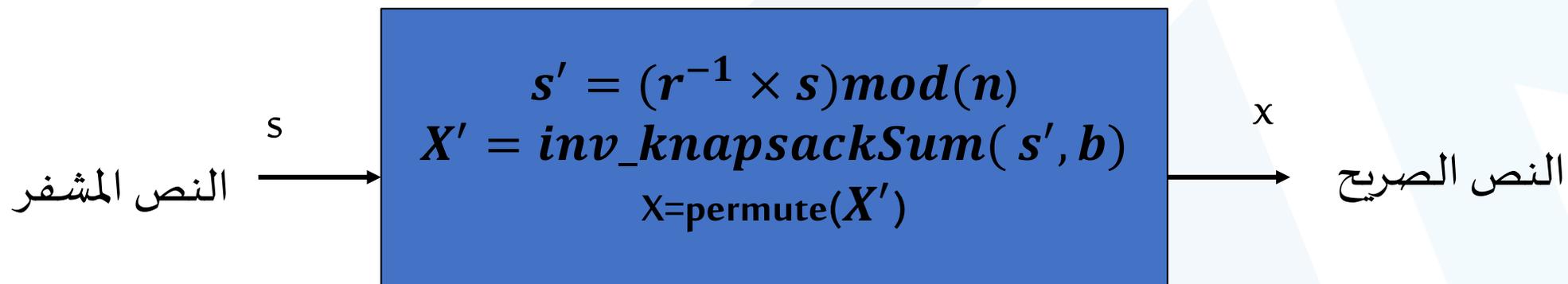
$$S2 = X_1 a_1 + X_2 a_2 + X_3 a_3 + X_4 a_4$$

$$S2 = 1 * 17 + 1 * 21 + 0 * 9 + 1 * 14 = 52$$

النص المشفر هو: 9 52

مراحل نظام تشفير حقيبة الظهر (3/4)

عملية فك التشفير ❖



المفتاح الخاص (b,n,r) والتدوير

المخطط الصندوقي

مراحل نظام تشفير حقيبة الظهر (4/4)

❖ خطوات عملية فك التشفير:

1. لعكس الضرب بـ r نوجد معكوس r بالنسبة لـ $\text{mod}(n)$

$$r^{-1} \text{mod}(n) = v$$

بحيث: $r \times v \equiv 1 \text{mod}(n)$

2. نحسب $s' = (r^{-1} \times s) \text{mod}(n)$

3. نعكس عملية ملء الحقيبة $X' = \text{inv_knapsackSum}(s', b)$

أي نكتب الجداء الذي نحصل من خلاله على القيمة s' اعتماداً على b و بذلك نحصل على قيم X' :

$$s' = X'_1 b_1 + X'_2 b_2 + \dots + X'_k b_k$$

4. ندور قيم X' وفق التدوير المفروض فنحصل على X .

مثال عن مرحلة فك التشفير في نظام تشفير حقيبة الظهر

1. معكوس $r=7$ بالنسبة لـ $\text{mod}(25)$ قيم المعكوس محصورة بين 1 حتى 24

$$7^{-1} \text{mod}(25) \equiv 18$$

بحيث: $7 \times 18 \text{ mod}(25) \equiv 126 \text{ mod}(25) = 1$

إذاً 18 هي معكوس 7 بالنسبة لـ $\text{mod}(25)$

2. نحسب $s' = (r^{-1} \times s) \text{mod}(n) = (18 \times 31) \text{mod} 25 = 558 \text{ mod} 25 = 8$

$$s' = X'_1 b_1 + X'_2 b_2 + X'_3 b_k + X'_4 b_k$$

3. لدينا $b = [2, 3, 6, 12]$ فيكون

$$8 = 1 \times 2 + 0 \times 3 + 1 \times 6 + 0 \times 12$$

فتكون قيم $X' = 1 \ 0 \ 1 \ 0$

4. ندور قيم X' وفق التدوير المفروض $[3, 2, 4, 1]$ فنحصل على $X = 1001$.

نهاية المحاضرة الثالثة