جامعة المنارة

كلية الهندسة

قسم المعلوماتية

Information System Security
أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

عناوين المحاضرة السادسة

➢ تابع البعثرة (Hash Function):

- ✓ مقدمة
- ✓ تعريف تابع البعثرة (Hash function)
- ✓ خصائص تابع البعثرة
- ✓ أهم استخدامات تابع البعثرة
- ✓ تصنيف تابع البعثرة

مقدمة إلى تابع البعثرة

- تعرف تكاملية المعطيات على أنها الخاصية التي تسمح بالتحقق من أن المعطيات لم تعدل من قبل كيان غير مخول له بذلك سواء بشكل مفاجئ أو مقصود.
- يستخدم تابع البعثرة (hash) عملياً من أجل التحقق من متطلب تكاملية المعطيات.

تعريف تابع البعثرة (Hash function)

- **تعريفه:**

هو تابع يربط قناة ثنائية ذات طول متغير مع قناة ذات طول ثابت.
رياضياً هو تابع حسابي فعال يحول السلاسل الثنائية ذات الأطوال المتغيرة إلى سلاسل ثنائية ذات أطوال ثابتة (n). نرمز له بـ h():

$$h:\{0,1\}^* \to \{0,1\}^n, m \to h(m)$$

- ✓ مثالياً تكون قيم n ما بين 128-256 bits
- ✓ تدعى قيمة خرج تابع البعثرة بموجز الرسالة (message digest)
- ✓ يطلق عليه أحياناً : تابع البصمة (fingerprint function) أو تابع التجزئة

خصائص تابع البعثرة (Hash Function) (1/5)

١. **الضغط (Compression):** يجب أن ينتج خرجاً بطول ثابت وأصغر مقارنة مع أطوال الدخل.

Message	*Message Digest*
4523AB1352CDEF45126	13AB
723BAE38F2AB3457AC	02CA
AB45CD1048765412AAAB6662BE	A38B

٢. **سرعة الحساب (Fast Computation):** يجب أن يكون سهل الحساب مهما كانت قيمة الدخل أي أن يكون من السهل حساب على قيمة h(m) من أجل قيمة دخل معلومة m

٣. **وحيد الاتجاه (One-way):** من أجل قيمة y معطاة من غير الممكن إيجاد x بحيث $h(x) = y$

خصائص تابع البعثرة (Hash Function) (2/5)

٤. **تأثير الانهيار الثلجي (Avalanche Effect) :** تغيير بسيط في دخل التابع يغير االخرج بشكل كبير

مثال: عند تطبيق تابع البعثرة SHA-256 :

SHA-256("Hello") = 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

SHA-256("hello") = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

نلاحظ تغيير بسيط على الدخل باستبدال H بـ h أعطى خرجاً مختلفاً تماماً

خصائص تابع البعثرة (Hash Function) (3/5)

5 .مقاوم للتصادمات (Strong collision resistance): أي من أجل أية قيمتين مختلفتين ينتج حكماً خرجين مختلفين: $y \neq x \rightarrow h(y) \neq h(x)$

تعريف مقاومة التصادم رياضياً:

بفرض أن تابع البعثرة يعطي على خرجه n بت، يكون عدد القيم الممكنة : $N = 2^n$

- عدد المحاولات اللازمة لإيجاد تصادم باحتمال معين p:

$$k \approx \sqrt{2N\ ln\left(\frac{1}{1-p}\right)}$$

صيغ هامة لعدد المحاولات :

$k \approx 1.1774\sqrt{N}\ ; P = 0.5$ $\quad$ $k \approx 2.146\sqrt{N}\ ; P = 0.9$

- الوقت المطلوب لإيجاد التصادم :

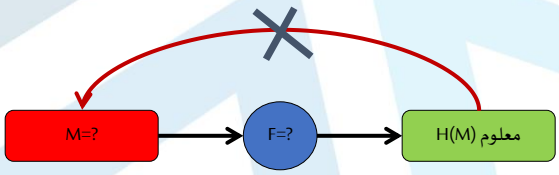
$$T(sec) = \frac{k}{V}$$

V : سرعة الحساب

خصائص تابع البعثرة (Hash Function) (4/5)

6 .مقاوم ضد هجوم الصورة الأولية (Pre-image Attack)

- من المستحيل إيجاد الدخل من الخرج
- إذا كانت قيمة التابع h(m) معروفة للمهاجم فإنه من الصعب حساب m



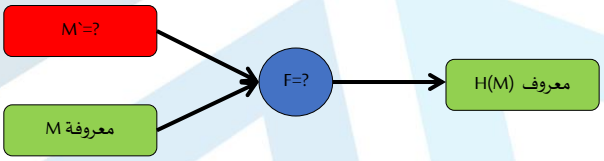
هذه الخاصية تحمي ضد المهاجم الذي يمتلك قيمة خرج تابع البعثرة ويحاول إيجاد قيمة الدخل

خصائص تابع البعثرة (Hash Function) (5/5)

7. مقاوم ضد هجوم الصورة الثانية (Second pre-image Attack)

- من المستحيل إيجاد دخل آخر غير الدخل الأصلي ويعطي نفس الخرج لتابع البعثرة
- من أجل قيم رسالة m و تابع البعثرة h(m) معروفة من قبل المهاجم ، فإنه من الصعب إيجاد رسالة أخرى **m`** بحيث يكون لها نفس قيمة تابع البعثرة :

أي من الصعب جداً تحقيق: hash(m)=hash(m`)



هذه الخاصية تحمي من المهاجم الذي يمتلك الدخل وقيمة خرج تابع البعثرة المو افق له ويريد أن يستبدل القيمة الأصلية بقيمة مختلفة كقيمة شرعية

تصنيف تو ابع البعثرة (1/2)

تصنف إلى نوعين أساسيين:

❖ **تو ابع بعثرة دون مفتاح :**

هي توابع البعثرة التي تمتلك دخل واحد هو الرسالة . مثال عنها **MDC (Manipulation Detection Code)**

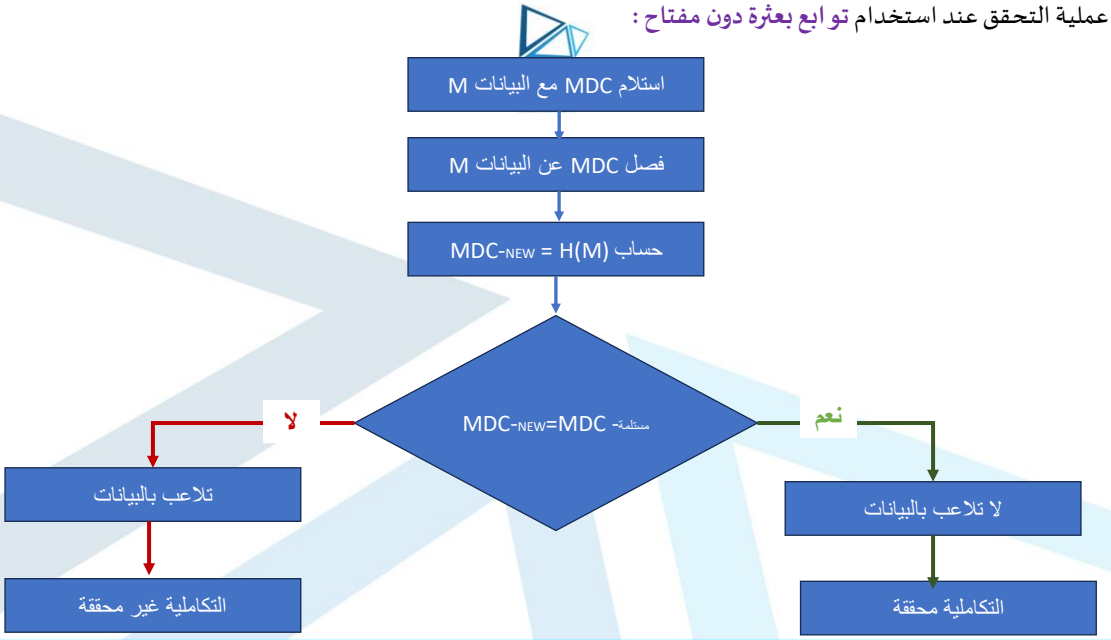
- في MDC : خرج تابع البعثرة ((H(M)يلصق مع المعلومات الأصلية (M) التي طبق التابع عليها ومن ثم تشفر بهدف الحماية من العبث فيها. أي يُرسل في قناة موثوقة كالآتي: $MDC = E_K(M \| H(M))$ حيث K هو المفتاح السري.

✓ **أهم استخداماتها** هي كشف التلاعب المتعمد مثل تزوير العقود الرقمية والبطاقات الذكية والسجلات الطبية والمستندات الموقعة الكترونياً

✓ **لكن لا تستخدم من أجل المصادقة**

✓ **من الأمثلة العملية عليها:** SHA-256, SHA-512, MD5

تكون عملية التحقق عند استخدام **توابع بعثرة دون مفتاح :**



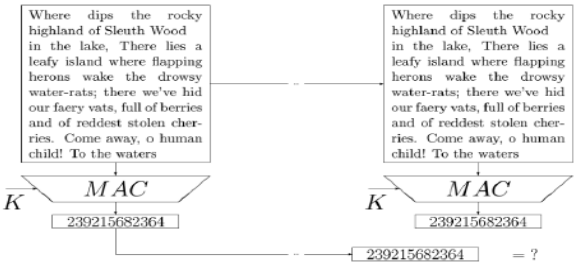
جامعة المنارة

تصنيف توابع البعثرة (2/2)

❖ **توابع بعثرة مع مفتاح :**

هي توابع البعثرة التي تمتلك **دخلين اثنين** أحد هما هو المفتاح السري و الآخر هو الرسالة.

مثال عنها (MAC(Message Authentication Code



تحسب الـMAC و يرسل الآتي: $M \| MAC_K(M)$

- K مفتاح سري مشترك

✓ **أهم استخداماتها** هي كشف التلاعب المتعمد إضافة إلى المصادقة

✓ **من أمثلتها العملية:** HMAC, CMAC, GMAC

Message Authentication Code (MAC)

➢ **آلية العمل:**

✓ يتشارك المرسل A والمستقبل B بنفس المفتاح السري

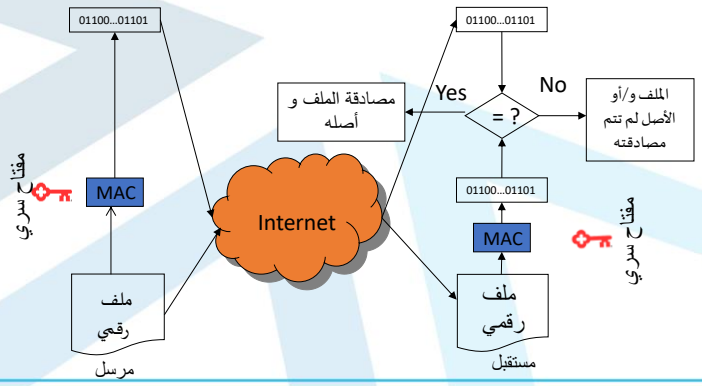
✓ يحسب المرسل $MAC_{K_{AB}}(m)$ و تلصق مع الرسالة (m) من أجل إرسالها باستخدام المفتاح السري K_{AB}

✓ يرسل المرسل $m \| MAC_{K_{AB}}(m)$

✓ بعد استقبال الرسالة، يبحث المستقبل عن مصدر الرسالة المستقبلة كما يلي:

- يعيد المستقبل حساب الـ $MAC_{K_{AB}}(m)$ للرسالة المستقبلة باستخدام المفتاح السري K_{AB}
- يقارن هذه النتيجة مع الـ $MAC_{K_{AB}}(m)$ المستقبلة ويحدد فيما كانت الرسالة المستقبلة أصلية و مرسلة من المصدر الصحيح أم لا

مصادقة أصل المعطيات باستخدام الـ MAC



مقارنة بين نوعي تابع البعثرة

الصنف	HMAC (MAC)	SHA (MDC)
الهدف الرئيسي	التكاملية والمصادقة	التكاملية
المفتاح	مفتاح متماثل (سري)	لا يوجد
من يمكنه الإنشاء؟	من يعرف المفتاح السري	أي شخص
من يمكنه التحقق؟	من يعرف المفتاح السري	أي شخص
حماية ضد	التلاعب + انتحال الهوية	التلاعب بالبيانات
الأداء	سريع	سريع
التوزيع	يحتاج توزيع آمن للمفتاح	لا يحتاج

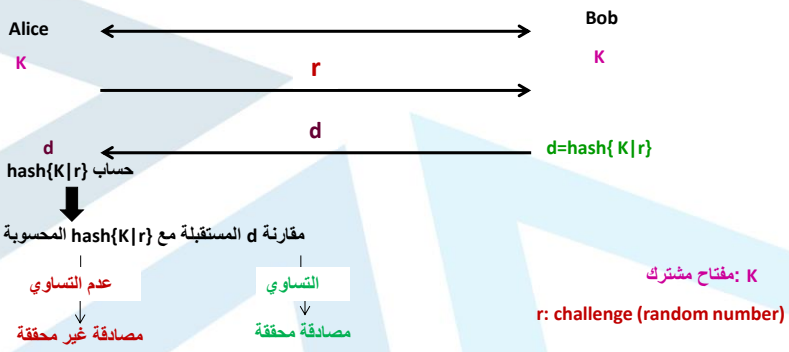
أهم استخدامات تابع البعثرة

١. تحقيق مصادقة أصل المعطيات
٢. تحقيق متطلب المصادقة
٣. تحقيق متطلب التكاملية

المصادقة باستخدام تابع البعثرة (1/2)

- في حال أراد طرفان التأكد من هوية كل منهما والتأكد من المفتاح المشترك بينهما
- يرسل أحدهما رقماً عشوائياً هذا الرقم العشوائي يكون بمثابة تحدي (challenge)
- الطرف الذي استقبل التحدي يطبق تابع البعثرة على قيمة هذه القيمة هي لصق لهذا التحدي مع المفتاح المشترك، و يرسل خرج تابع البعثرة الناتج إلى الطرف الآخر .
- عندما يستقبل ذلك الطرف خرج تابع البعثرة يعيد حساب تابع البعثرة باستخدام الرقم العشوائي والمفتاح المشترك ، ويقارن النتيجة مع تابع البعثرة التي استقبلها .
- هنا نميز حالتين:
  - ✓ في حال التساوي تكون المصادقة محققة
  - ✓ في حال عدم التساوي تكون المصادقة غير محققة

المصادقة باستخدام تابع البعثرة (2/2)



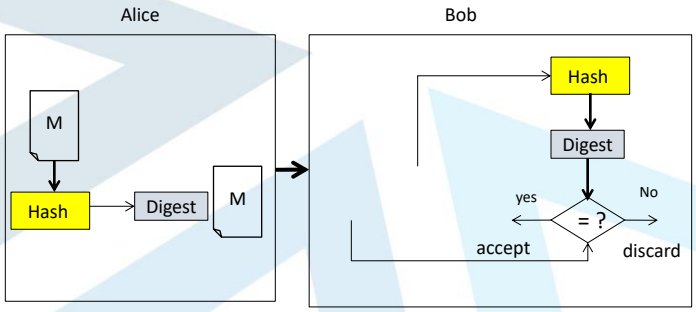
تكاملية البيانات باستخدام تابع البعثرة (1/2)

- الغاية من استخدام تابع البعثرة هنا التأكد من أن الرسالة الأصلية لم تعدل، ولكن لا يضمن التحقق من أصل المرسل
- يطبق المرسل تابع البعثرة على الرسالة ومن ثم يرسل خرج التابع ملصقاً مع الرسالة
- في جهة الاستقبال يحسب المستقبل تابع البعثرة للرسالة الواصلة إليه ويقارن الناتج مع قيمة تابع البعثرة المستقبلة

❖ في حال التطابق الرسالة صحيحة لم تتعرض للتعديل ومتطلب التكاملية محقق

❖ في حال عدم التطابق الرسالة معدلة ومتطلب التكاملية غير محقق

تكاملية البيانات باستخدام تابع البعثرة (2/2)



جَامعة المَنارة
MANARA UNIVERSITY

نهاية المحاضرة السادسة