الجمهورية العربية السورية
جامعة قرطبة الخاصة
كلية الهندسة / تكنولوجيا هندسة الاتصالات والمعلومات

ملخص محاضرة خاصة بمقرر مادة
"أمن ووثوقية معلومات"
للفصل الثاني للعام الدراسي 2020/2019

الغوريتم هاش الآمن
Secure Hash Algorithm (SHA)

I. ما هو الغوريتم هاش Hash Algorithm:

إن دالة التجزئة Hach function هي نوع من الوظائف الرياضية التي تحول البيانات Data إلى بصمة "فريدة Fingerprint "unique لتلك البيانات تسمى "التجزئة Digest".

- **خصائص الغوريتم هاش:**

تابع تجزئة التشفير Hash له الخصائص الرئيسية التالية:

1. **وحيد:** وهذا يعني أن نفس الرسالة تؤدي دائمًا إلى نفس التجزئة Digest

H (x) is **unique**

2. **ذو طول ثابت fixed length:** وهذا يعني أن الخرج Digest له دوماً نفس الطول مهما كان طول الرسالة

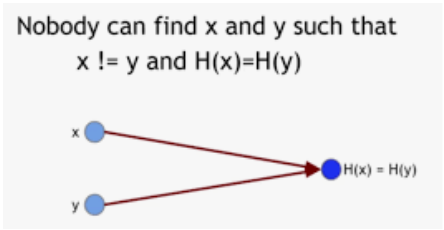
The **Input** can be of **any length**, but **output** has a **fixed** length

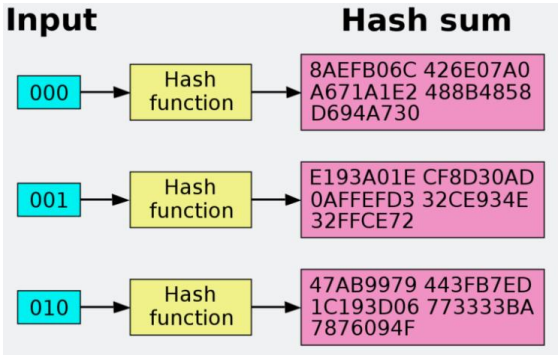
3. **غير عكسيone-way:** وهذا يعني أنه لا يمكن الحصول على أصل الرسالة من خرج التجزئة Digest

H (x) is **one-way**

4. **عديم التصادم collision-free:**

H (x) is **collision-free**





الشكل (1) خصائص Hash

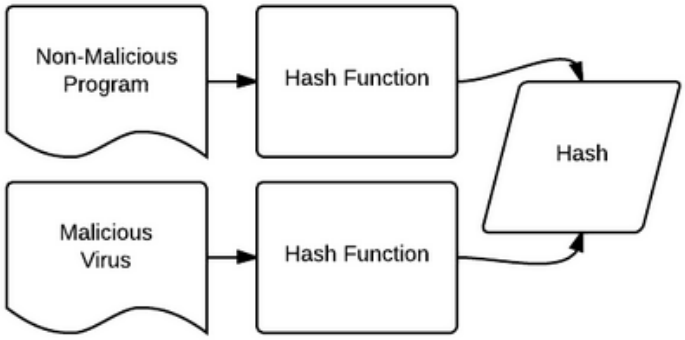
5. سريع وسهل الحساب قيمة التجزئة لأي رسالة معينة:

H (x) is **easy** to compute for a given value x

• ما هو التصادم Collision:

ـ **تعريف التصادم**: هو الحالة الذي يحدث عندما يكون لقطعتين مختلفتين من البيانات نفس قيمة التجزئة Hash أو المجموع الاختباري Checksum أو بصمة الإصبع أو ملخص التشفير:

$$H(x1) = H(x2)$$



الشكل (2) آلية عمل التصادم Collision

نظرًا للتطبيقات المحتملة لوظائف التجزئة في إدارة البيانات وأمن الكمبيوتر ، أصبح تجنب التصادم Collision موضوعًا أساسيًا في علوم الحاسب.

• هجوم هاش التصادمي Hash Collision Attack:

هجوم التصادم لتابع هاش هو محاولة للعثور على سلسلتي إدخال x1, x2 لدالة التجزئة Hach ينتجان نفس نتيجة التجزئة:

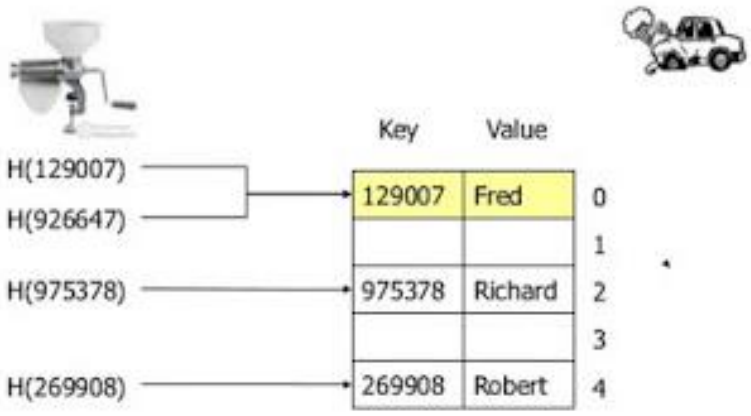
$$H(x1) = H(x2)$$

ـ **تعليل إمكانية حدوث الهجوم**: نظرًا لأن وظائف التجزئة Hash لها طول إدخال لا نهائي وطول إخراج محدد مسبقًا ، **سيكون** هناك حتمًا **إمكانية** إدخالين مختلفين ينتجان نفس تجزئة الإخراج.

• مقاومة التصادم Hash Collision Attack-Resistace:

مقاومة التصادم خاصية من وظائف التجزئة المشفرة SHA! (سنتعرف عليها لاحقاً)

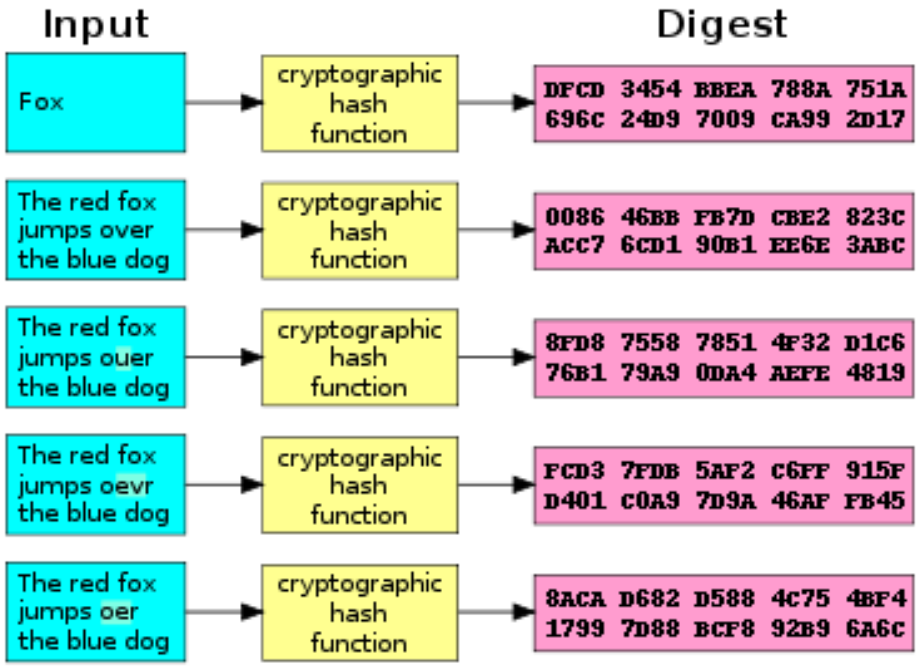
وظيفة التجزئة مقاومة للتصادم إذا كان من الصعب العثور على اثنين من المدخلات التي تجزئة إلى نفس الناتج ؛ أي ، مدخلين a و b بحيث H (a) = H (b). كل وظيفة تجزئة ذات مدخلات أكثر من المخرجات سيكون لها بالضرورة تصادمات!



الشكل (3) آلية عمل

• **خصائص إضافية:**

- لا يمكن إنشاء رسالة تعطي قيمة تجزئة معينة
- لا يمكن العثور على رسالتين مختلفتين بنفس قيمة التجزئة
- إن أي **تغيير بسيط** في رسالة سيؤدي إلى **تغيير** قيمة التجزئة **على نطاق واسع** بحيث تظهر قيمة التجزئة الجديدة غير المرتبطة بقيمة التجزئة القديمة:

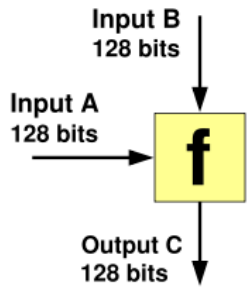


الشكل (4) ثبات طول خرج تابع Hash

• **تصميم وظيفة التجزئة Hash function design**

- طريقة (بناء ميركل – دامغارد Merkle–Damgård construction):

تكون دالة التجزئة Hash function في هذه الطريقة قادرة على **تحويل** أي رسالة Message مهما كان طولها إلى **خرج ذي طول ثابت** Fixed-Length Output. يتم الحصول على ذلك بتطبيق تابع "ضغط المعطيات وحيد الاتجاه" One-way Pressure Function (انظر الشكل).

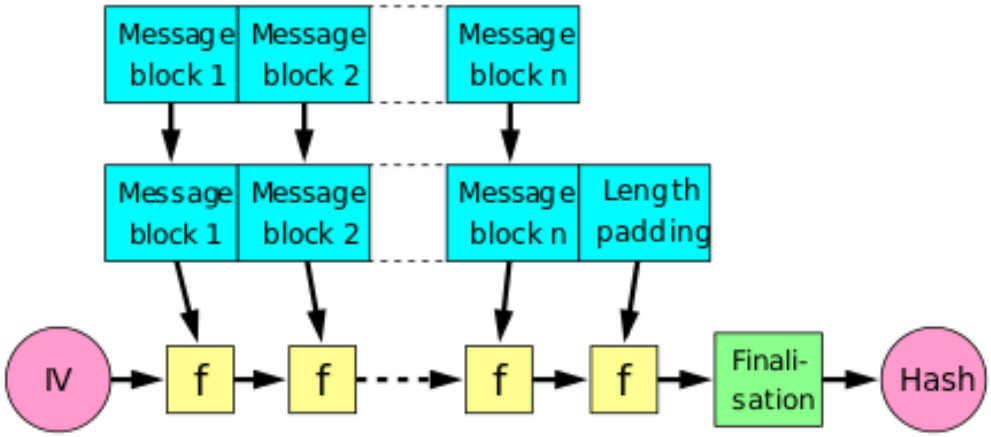


الشكل (5) مثال عن آلية عمل تابع "ضغط المعطيات وحيد الاتجاه" One-way Pressure Function

- خطوات تنفيذ (بناء ميركل – دامغارد Merkle–Damgård construction):

1. يتم **تقسيم الدخل إلى سلسلة من البلوكات متساوية الطول** (block 1, block 2, ...block n)
2. يتم تطبيق **"وظيفة ضغط المعطيات أحادية الاتجاه"** one-way compression function
3. يتم حساب طول الحشو اللازم Length Padding وتطبيق **وظيفة ضغط المعطيات** عليه

وبالتالي الحصول في نهاية المطاف على خرج Output له نفس الطول (نفس عدد bits) هو تابع هاش Hash كما هو مبين بالشكل:



الشكل (6) آلية عمل Hash حسب طريقة بناء Merkle-Damgård

• ملاحظات:

- إن عملية الضغط إما أن تكون مصممة خصيصًا للتجزئة Hashing أو يتم بناؤها من بلوك التشفير block cipher.
- إن المميزة الأساسية لوظيفة التجزئة Hach المنفذة بطريقة بناء Merkle-Damgård هي كونها مقاومة للتصادم collision.

II. ما هو الغوريتم هاش الآمن Secure Hash Algorithm (SHA) :

هو نسخة آمنة لألغوريتم هاش Hash Algorithm تم نشره من قبل المعهد الوطني الأمريكي للمقاييس والتكنولوجيا National Institute of Standards and Technology (NIST).

• إصدارات الغوريتم هاش الآمن:

1. **SHA-0 :** وهو تعديل عن نسخة 160-bit hash المنشورة عام 1993

2. **SHA-1 :** وهو أيضاً 160-bit hash تعديل عن Message-Digest algorithm(MD5) الذي يستخدم 128-bit hash المصمم من قبل وكالة الأمن القومي الأمريكي National Security Agency (NSA) ليكون بمثابة التوقيع الرقمي Digital Signature. لم يعد معتمد بعد عام 2010

3. **SHA-2 :** صمم من قبل وكالة الأمن القومي الأمريكي National Security Agency (NSA) عام 2001 بأحجام بلوكات Block Size مختلفة أشهرها SHA-256 and SHA-512.
- يشتهر **SHA-2** أيضاً باسم **SHA-256**
- يعتبر SHA-256 واحد من أهم عائلة *-SHA (يشار إليه أيضاً باسم SHA-2) كم يعتبر من **أقوى** وظائف التجزئة Hash functions المتاحة. ولم يتم اختراقه بأي طريقة.

4. **SHA-3 :** تم اختياره عام 2012 في مسابقة دولية للمصممين من خارج وكالة الأمن القومي الأمريكي National Security Agency (NSA). له أحجام بلوكات Block Size مختلفة أشهرها SHA-256 and SHA-512

• استخدامات الغوريتم هاش الآمن:

يعتبر SHA أحد مكونات شهادة SSL المستخدمة لضمان عدم تعديل البيانات. يحقق SHA ذلك من خلال إيجاد بصمة التشفير Digest وأي تغيير في جزء معين من البيانات سيؤدي إلى قيمة تجزئة مختلفة. نتيجة لذلك ، تعد قيم التجزئة المختلفة هي معيار تحديد ما إذا تم تغيير البيانات.

- إن *-SHA **لا تحتاج** إلى **مفتاح** Key ، فهي فقط تحسب قيمة التجزئة Digest من أي إدخال Input.

- **مقارنة هاش الآمن Comparison of SHA functions:**

Functions	Another Name	Message Digest Size	Word Size	Steps Number
DM5	DM5	120	32	64
SHA-0	SHA-0	160	32	80
SHA-1	SHA-160	160	32	80
SHA-2	**SHA-256**	**256**	**64**	**64**
SHA-3	SHA-512	512	64	80

جدول (1) مقارنة هاش الآمن SHA functions

III. شهادة المفتاح العام Public key certificate (SSL/ TLS certificate):

- **تعريف شهادة المفتاح العام Public key certificate:**

شهادة المفتاح العام أو شهادة رقمية أو شهادة هوية هو أحد مُصطلحات علم التشفير، وهي عبارة عن **وَثيقة إلكترونية تستخدم لإثبات ملكية المفتاح العام**، حيثُ تشمل الشَهادة معلومات عن المَفتاح وعن هوية صاحبه بالإضافة إلى التوقيع الرقمي بهدف التأكد من صِحة مضمون الشَهادة.

- يتم ذلك بواسطة البروتوكولين التاليين:

1. **بروتوكول Secure Sockets Layer (SSL)** "طبقة المقابس الآمنة" وهو النسخة الأقدم والذي تم إهماله الآن.
2. **بروتوكول Transport Layer Security (TLS)** "أمان طبقة النقل" وهو بروتوكول آمن تم تطويره لإرسال المعلومات بشكل آمن عبر الإنترنت (لتوفير الخصوصية أمان الاتصالات)

- تستخدم العديد من مواقع الويب بروتوكول TLS/ SSL في مواقعها مثل صفحات حساب المستخدم والخروج عبر الإنترنت .

- عادةً عندما يُطلب منك "**تسجيل الدخول** Log in" على موقع ويب، يتم تأمين الصفحة الناتجة بواسطة بروتوكولي طبقة المقابس الآمنةSSL و أمان طبقة النقل TLS

- **الفرق بين بروتوكولي (SSL/ TLS):**

- أمان طبقة النقل (TLS) هو البروتوكول اللاحق لبروتوكول SSL وهو **نسخة محسنة** منه يعمل بنفس طريقة SSL، باستخدام التشفير لحماية نقل البيانات والمعلومات.

- غالبًا ما يتم استخدام المصطلحين بالتبادل

- إذن الفرق بين TLS وSSL ليس كبير. معظمنا على دراية SSL طبقة مآخذ التوصيل الآمنة ولكن ليسTLS أمان طبقة النقل "أي ذو شهرة أكبر"، ومع ذلك فإن كلاهما بروتوكول يستخدم لإرسال البيانات عبر الإنترنت بأمان

- SSL أقدم من TLS ولكن يمكن لجميع شهادات SSL استخدام تشفير SSL وTLS

- **الغاية من استخدام بروتوكولي (SSL/ TLS):**

السبب الرئيسي لاستخدام SSL هو **الحفاظ على المعلومات الحساسة** المرسلة عبر الإنترنت **مشفرة** بحيث يمكن **للمستلم المقصود فقط** الوصول إليها

- عند استخدام شهادة طبقة المقابس الآمنة، تصبح المعلومات **مشفرة** و**غير قابلة للقراءة** للجميع باستثناء الخادم الذي تقوم بإرسال المعلومات إليه

- يتم استخدام SSL/ TLS في كل مستعرض browser في جميع أنحاء العالم لتوفير وظائف https (آمنة HTTP)

• طبقة بروتوكولي (SSL/ TLS) في OSI:
كلاهما يعمل في طبقة التقديم في نظام OSI (الطبقة السادسة Layer6)

V. المجموع الاختباري Checksum:

المجموع الاختباري Checksum هو من أساسيات وظائف تابع التجزئة Hash Function والتي يمكن استخدامها **للكشف** عن العديد من **أخطاء تلف البيانات والتحقق** من **تكامل البيانات** بشكل عام

• الفرق بين Checksum و Hash:
الغرض من المجموع الاختباري Checksum هو التحقق من سلامة البيانات وتحديد أخطاء نقل البيانات ، في حين تم تصميم التجزئة لإنشاء بصمة رقمية فريدة للبيانات.

• استخدامات Checksum:
المجموع الاختباري هو **قيمة عددية تمثل عدد البتات bits في رسالة نقل** يستخدمها متخصصو تكنولوجيا المعلومات لاكتشاف الأخطاء عالية المستوى في عمليات نقل البيانات قبل الإرسال، يمكن تعيين قيمة المجموع الاختباري لكل جزء من البيانات أو الملفات بعد تشغيل وظيفة تجزئة التشفير Hash function.

• معيار نجاح Checksum:
بما أن المجموع الاختباري Checksum هو طريقة للكشف عن الأخطاء في جهاز الإرسال، لذلك **تُحسب القيمة العددية للإرسال** (وفقًا لعدد البتات المحددة أو غير المحددة في رسالة) وتُرسل مع كل إطار رسالة... في حالة **تطابق قيمة المجموع الاختباري المُستَلَم مع القيمة المرسلة** ، يعتبر الإرسال **ناجحًا وخاليًا من الأخطاء** Error-Free.

***