جمهورية العراق / وزارة التعليم العالي والبحث العلمي
جامعة القادسية / علوم الحاسوب وتكنولوجيا المعلومات
قسم الحاسوب

نظام تشفير بإستخدام شفرة md5

بحث تقدمت به الطالبات

(حنان مجيد عبد - رقيه علي حمزة - زهراء كاظم محمد)

الى كلية علوم الحاسوب وتكنولوجيا المعلومات / قسم الحاسوب وهو
جزء من متطلبات نيل شهادة البكالوريوس في علوم الحاسوب

إشراف الاستاذ

علاء عبد المحسن

١٤٣٨هـ ٢٠١٧ م

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

(سَنُرِيهِمْ آيَاتِنَا فِي الْآفَاقِ وَفِي أَنْفُسِهِمْ
حَتَّى يَتَبَيَّنَ لَهُمْ أَنَّهُ الْحَقُّ أَوَلَمْ يَكْفِ
بِرَبِّكَ أَنَّهُ عَلَى كُلِّ شَيْءٍ شَهِيدٌ)

صدق الله العظيم

من سورة فصلت:الأية ٥٣

الإهداء:

إلى من جرع الكأس فارغاً ليسقيني قطرة حب

إلى من كلّت أنامله ليقدم لنا لحظة سعادة

إلى من حصد الأشواك عن دربي ليمهد لي طريق العلم

إلى القلب الكبير

(والدي العزيز)

إلى من أرضعتني الحب والحنان

إلى رمز الحب وبلسم الشفاء

إلى القلب الناصع بالبياض

(والدتي الحبيبة)

إلى القلوب الطاهرة الرقيقة والنفوس البريئة إلى رياحين حياتي

(إخوتي)

شكر وتقدير

انطلاقا من العرفان بالجميل ،فأنه ليسرنا ويثلج صدرنا أن نتقدم بالشكر والامتنان إلى أستاذنا ،ومشرفنا الدكتور (علاء عبد المحسن) الذي مدنا من منابع علمه بالكثير،والذي ماتوانئ يوما عن مد يد المساعدة لنا وفي جميع المجالات ،وحمدا لله بأن يسره في دربنا ويسر به أمرنا ،

وعسى أن يطيل الله في عمره ليبقى نبراسا متلألئا في نور العلم والعلماء .

وأتقدم كذلك بجزيل الشكر إلى كليتنا الحبيبة

متمثلة بعميدها الدكتور (د . هشام البيرماني) لكل ماقدمته لنا من مساعدة ومساندة مكنتنا من المضي بخطى ثابتة في مسيرتنا العلمية .

كما أتقدم بجزيل الشكر إلى أساتذتي أعضاء لجنة النقاش الموقرين على ما تكبدوه من عناء في قراءة هذا البحث المتواضع و أغنائها بمقترحاتهم القيمة .

المحتويات

الفصل الأول

1.1 MD5 أو خوارزمية خلاصة الرسالة 5 (Message-Digest 5)

تُعد دالة هاش تشفيرية (Message Digest) من أكثر دوال الاختزال انتشارًا، وقد صُمّمت في نسختها الأوليّة (MD2) عام 1989م عن طريق الدكتور رونالد ريفست أستاذ الحاسب في معهد ماساتشوستس للتقنية (MIT)، وتم تطويرها إلى نسخة (MD5) عن طريق مطوّرها نفسه عام 1991م بعد أن تمّت دراسة خواصّ الأمن فيها وتغطية ثغرات سابقتها لفترة طويلة. تستخدم MD5 دالّة ميركل ديمقارد (Merkle–Damgård construction)، وتقوم على اختزال رسالة ذات طول متغيّر إلى طول ثابت هو 128 بت بغضّ النظر عن طولها الأصليّ، حيث يتم تحويل الرسالة [1]إلى حزم (blocks) طول كُلّ منها 512 بت بغرضِ اختزالها في خطواتٍ لاحقة. من الجدير بالذكر أنّ أي تغيير مهما كان حجمه في النصّ الأصليّ يُنتج قيمة اختزال مختلفة تمامًا عن القيمة السابقة، أو هو ما تحاول الدالّة تحقيقه خلاص.

1.2 خواص خوارزميّة التشفير MD5

تتميّز MD5 عن غيرها من دوال الاختزال في عدّة نقاط:

1.سهلة التنفيذ وقليلة التكلفة.

2. تُوفّر مخرجًا مختلفًا لكلّ مدخل مهما صغر الفرق بينهم وهو ما يُسمّى بالبصمة fingerprint

3. استحالة الرّجوع من قيمة الاختزال إلى الرسالة الأصليّة.

1.3 خطوات عمل خوارزميّة التشفير MD5

1. إضافة الحشو Padding): في هذه الخُطوة نقوم بإسناد أجزاء (bits) إضافيّة للنّص الأصليّ، ويتم ذلك [1]في مرحلتين:

أ. نبدأ بإضافة 1 ثُم نملأ البقيّة بالأصفار حتّى يصبح طول الرسالة منسجمًا مع 448 % 512 (أي أننا نُضيف حتّى يُصبح الطّول أقل ب 64 بت من أن يقبل القسمة على 512).

ب. إضافة طول الرسالة: 64 بت تُضاف لنهاية الرسالة تُحدّد طولها الأصليّ بالبايات (Bytes) بعد تحويل الرقم إلى صيغته الثنائيّة (Binary). في حال كانت الرسالة طويلة جدًا وكان التمثيل الثنائي لعددها أكثر من 64 بت، فإنّ الأجزاء ذات الترتيب المنخفض (low-order bits) هي التي تُستخدم فقط. بعد هذه الخطوة يُصبح طول الرسال 512 س، حيث س هو أي عدد موجب.

2. التقسيم (Partition): يتم في هذه الخطوة تقسيم الرسالة إلى حزم طول كل حزمة منها 512 بت.

3. تعريف المساحة التخزينيّة (Initialize MD Buffer): يتم فيها تعريف مساحة بطول 4 كلمات (four-word buffer) طول كل واحدة منها 32 بت، تُعرّف مسبقًا بالقيم التالية:

A: 01 23 45 67

B: 89 ab cd ef

C: fe dc ba 98

D: 76 54 32 10

4. التنفيذ (Processing): ابتداءً نُعرّف 4 دوال مساعدة تأخذ كل منها مدخلاً مكوّنًا من 3 كلمات، كل كلمة عبارة عن 32 بت، وتُخرج كلمة واحدة مكوّنة من 32 بت أيضًا.

F(X,Y,Z) = XY v not(X) Z

(G(X,Y,Z) = XZ v Y not(Z

H(X,Y,Z) = X xor Y xor Z

((I(X,Y,Z) = Y xor (X v not(Z

تمرّ كل حزمة من البيانات بِأربع جولات (4 rounds) متتالية، تتكوّن كل جولة منها من 16 خطوة. نستخدم في كل خطوة جدولاً مُكوّنًا من 64 خانة 64 ... 1]T[يتم حسابها عن طريق دالّة sine وتساوي i)Sin(aps times 4294967296 =T[i]) حيث تحسب i بالراديان.

نقوم بتطبيق المعادلة التالية في كل خطوة:

a = b + ((a + g(b,c,d) + X[k] + T[i]) <<<s)

حيث إنّ:

g هي إحدى الدّوال المساعدة سابقة الذكر.

العمليّة + هي عمليّة الجمع % 32^2 (=% 4294967296)

a,b,c,d هي المساحات التخزينيّة المعرفة، وتُستخدم بترتيب محدّد في كل خطوة.

<<<s هي مقدار واتجاه الإزاحة (shifting)؛ إزاحة إلى اليسار بمقدار s.

[X[k] = M[i*16+k حيث k تتغيّر من 0 .. 15 في كل خطوة.

تُطبّق هذه المعادلة 16 مرّة في كل جولة، ثُم تكون مُدخلاً للجولة القادمة وهكذا.

5. المُخرجات (Output):

تُخرج هذه الدالّة المخرجات في A,B,C,D بالترتيب ابتداءً بالبت الأقل رتبة في A إلى الأعلى رتبة في D.

1.4 تطبيقات خوارزمية التشفير MD5

1. التأكيد على صحّة الملفّات (Data Integrity):

أحد أبرز أهداف دوال الاختزال بشكل عام التأكد من صحّة الملفّات المستلمة عن طريق قنوات الإرسال غير الآمنة، تعمل دالّة MD5 مثل نظيراتها من دوال التشفير على اختزال كامل الرسالة إلى قيمة اختزال نهائيّة، ترسل مع الرسالة فتُمكّن المستقبل عند اختزاله الرسالة مُجدّدًا بعد استلامها من التأكّد من كونها لم تُعدّل أو تعطب في الطريق. [2]

2. علم التوقيع الرقمي (Digital Signature):

هي ملفّات تُرسل مع الرسائل المُشفّرة أو غير المشفّرة بغرض إثبات هويّة المُرسل، حيث تضمن لنا ألاّ يقوم الأشخاص غير المخوّلون بانتحال شخصيّة أخرى موثوقة. ونظرًا لكون التواقيع الرقميّة تعتبر معرّفات لمستخدمها؛ فإنه ينبغي أن نضمن عدم وجود أكثر من توقيع يملك الرّقم ذاته، وهذه إحدى المشاكل التي تواجه علم الاختزال ويُطلق عليها مشكلة يوم الميلاد.

تضمن MD5 تفرّد قيمة الاختزال في مجال قدره 2^64 والذي عُدّ رقمًا مناسبًا لاستخدام التواقيع الرقمية حتّى تم اختراقها.

3. كلمة المرور (استيقان) (Authentication) :(Password)

من أجل الحفاظ على خصوصيّة المستخدمين، سواءً في الشركات أو الأجهزة الشخصيّة، فإنّ كلمات المُرور تُخزّن مُختزلة في قاعدة البيانات للحدّ من استفادة الشخص المُخترق منها إن أمكنه الوصول إليها، وتُعتبر MD5 أكثر دوال الاختزال استخدامًا في مجال كلمة المرور وتعريف المستخدم في الوقت الحاليّ.

1.5 كسر خوارزمية التشفير MD5

جرت الكثير من المحاولات لكسر هذه الخوارزمية عن طريق brute force attack على سبيل المثال، ولكن باء أكثرُها بالفشل بينما نجح البعض منها نجاحًا جُزئيًا حتى تم اختراقها وأُعلن أنّه يجب إيقاف استخدامها للملفّات المهمة والتواقيع الرقميّة في السنوات القريبة الماضية:

1. في عام 2004 استطاع العالمان Xiaoyun Wang و Hongbo Yu إيجاد تصادم في هذه الخوارزميّة، عن طريق إيجاد حزمتين مختلفتين تصلان لنفس قيمة الاختزال، وقد تم نشرها في ورقة بحث بعنوان: كيفيّة خرق MD5 ودوال الاختزال الأخرى

2. في عام 2007 طوّر مارك ستيفنز في رسالته الماجستير طريقة لاختراق MD5 عُرفت باسم: اصطدام البادئة المُختارة (chosen-prefix collisions)، تستغرق ما بين 15 إلى ساعة لتصنيع الاصطدام في أجهزة الكمبيوتر العاديّة

1.6 أوجه القصور في عملية التشفير

تنقسم أوجه القصور في عملية التشفير إلى ثلاثة أنواع:

1- الأخطاء البشرية.

2- أوجه الخلل في الشفرة ذاتها.

3- عمليات الهجوم غير المنطقية.

الفصل الثاني

2.1 دالة الهاش

هي دالة تأخذ مدخل بأي طول وتخرج نص له طول معين على حسب الدالة، فسواء كانت وأجدادها القديمة مثلMD4 ، أو كانت ال SHA بأنواعها SHA1 و SHA2 وحتى ايضاً هناك RIPEMD وهي دالة هاش معروفة ايضاً. الجدول التالي يبين انواع الخوارزميات المختلفة

Algorithm	Creator	Length (Bits)	Related standard
MD5	Ronald Rivest	128	RFC 1321
SHA-1	NSA and published by NIST	160	FIPS Pub 180
SHA-2	NSA and published by NIST	224 256 384 512	FIPS Pub 180-2 FIPS Pub 180-3 FIPS PUB 180-4
RIPEMD-160	Hans Dobbertin	160	Open Academic Community
SHA-3	Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche	224, 256, 384, 512	FIPS-180-5

المدخل هو اي binary data سواء كانت ملف ، باسورد، صورة، Imageمن القرص الصلب، وبشكل اساسي يمكنك أن تقول اي بياناتcontinuous/stream digital input

لاحظ اسم الدالة one way function أي أنه لا يمكن الرجوع ابداً من الهاش الناتج واستخراج البيانات الأصلية، وايضاً نظرياً لا يمكن ان تجد بيانات مختلفة لها نفس الهاش.. اخيراً اي تغيير ولو bit واحد في المدخل سوف يؤدي لناتج مختلف تماماً عن ما سبق

1. اختبار التكامل أو عدم حدوث تغيير في البيانات وهذا يسمى :Integrity فمن خلال ال Hashing لأي بيانات سوف تحصل على الهاش المخرج، في حال قمت بأخذ الهاش لنفس البيانات يجب أن تحصل على نفس الهاش الناتج، اذا تغير الهاش فهذا يعني أن البيانات قد تغيرت..

مثلاً لدى ملف واريد مراقبته هل تم تغييره أم لأ، فأسهل طريقة أحسب الهاش للملف، وفي اي وقت أخر اقوم بفحص القيمة بما هو مخزن وهكذا سوف أعرف هل تم التغيير عليه أم لأ..

مثال اخر عندما تحمل بعض البرامج من الانترنت سوف تجد بجانب زر التحميل الهاش لذلك الملف حتى بعدما ان تقوم بتحميله يمكنك ان تتأكد من صحة الملف وأنه وصل لك كما في الموقع

2. البحث :Searching فمثلاً اريد البحث عن الملفات المتشابه في قرص، فأسهل طريقة هي حساب هاش كل ملف، ومعرفة الهاشات المتطابقة وهكذا سوف اعرف ان هذه الملفات متطابقة لأن لها نفس الهاش، والذي نظرياً لا يمكن أن يكون لأي ملفين مختلفين نفس الهاش

هذا يتضمن ال Blacklist Searching مثلاً لدي مجموعه من الملفات (صور مخلة، ملفات منتشره مشتبه بها) و اريد البحث عنها في قرص معين، سوف احسب الهاش لتلك الملفات وابحث عليها داخل اي وسيط وبالتالي يمكن ايجادها بسرعه.

وايضاً يتضمن ال WhiteList Searching فمثلاً أريد البحث في ملفات في قرص النظام ولكن اريد أن يتجاهل ملفات معينة مثلاً ملفات ال dll الخاصة بالنظام وغيرها من الملفات المعروفة أنها تأتي مع النظام، فسوف احسبها واخزنها في قاعدة بيانات، وبالتالي عندما أبحث و اجد اي ملف له هذا الهاش فسوف اتجاهله لأنه ملف نظام وأنا اعرفه وهذا سيقلل وقت البحث والملفات التي تريد البحث حولها.هذه الطرق تستخدم في بعض برامج مكافحة الفيروسات، فمثلاً هناك ملفات فيروسية تكون معروفه وبالتالي اذا لديك قاعدة بيانات من الهاش لتلك الفيروسات تستطيع ببساطة البحث عنها في القرص ومقارنه اي ملف بالهاش في القاعدة واذا وجدته فهذا يعني انك وجدت فايروس ، طبعاً في الأنتي فابروس هذه ليست الطريقة الوحيدة على ايه حالة

3. تخزين البيانات بشكل غير قابل للاسترجاع :فكما هو معروف انه يجب تخزين كلمات السر في القاعدة على شكل Hashing والسبب أنه اذا حصل اختراق للقاعدة فسوف يتم جلب كل الباسوردات بسهوله، لذلك كان الأمر كتصعيب للمخترق، وبالتالي اي مستخدم يسجل لديك سوف تخزنه باسورده كهاش، وعندما يسجل دخول سوف تأخذ الباسورد وتحسب الهاش فاذا تطابق مع ما يوجد في القاعدة فسوف تتأكد من صحة الباسورد وبالتالي تسمح له بالدخول

بالنسبة للعيوب أو الهجمات (ما يعرف بكسر الشفرات) فالحاصل أنه لا يتم ذلك ولا توجد اي طريقة لذلك الا من خلال حسابات مسبقة أو وجود تصادم في البيانات:

Collision attack

Preimage attack

المشكلة الأولى هي أن بعض الخوارزميات كشفت بها ضعف وبالتالي امكن ايجاد مدخلين مختلفين لهم نفس الهاش ، وهذا يسمى Collision ، وخوارمية ال MD5 اشهر من تعرضت لهذه الهجمة

لذلك الأفضل أن تستخدم SHA2 سواء 265 أو حتى 512 بت) وحتى ال SHA-1 قد تعرضت لمثل هذه الهجمات.

احتمال ايجاد اي Collision هو قليل جداً، فمثلاً في ال SHA-1 احتمال ايجاد تصادم واحد يكون بين كل 2 اس 80 رسالة وهو رقم كبير جداً ولا يستطيع ان يقوم به اي جهاز عادي.

اما المشكلة الثانية هي أن منها الفكرة أنه يتم توليد هاشات لأي نصوص سواء كانت عشوائية أو يتم سحبها من اي قاعدة بيانات أو حتى عن طريق عمل crawling على الويب والمنتديات وسحب ال textual information ويمكن أن تكون بدايه للبيانات، وحساب هذه النصوص وما يقابله من الهاش وتخزينها على جداول في قاعدة بيانات ما (هذه الجداول في العادة تسمى Rinbow Tables)، وبالتالي اذا حصلت على هاش معين وصدف انه محسوب من قبل فسوف تجد النص الأصلي له ، ايضاً هناك من يقوم بعملية حساب الهاش بالاستفادة من قدرات المعالجة الحديثة Multi-Coresويقوم بتوليد الهاشات بكل ال coresالمتاحة، وهناك من يستخدم ال GPU داخل كرت الشاشه للقيام بذلك ، وهناك من يقوم بالعملية على Distributed Systems وفي النهايه كلهم يقوموا بالتخزين على أمل ان يصدف الهاش بها، ولكن اذا كانت كلمة المرور معقدة فسوف يصعب ذلك اخيراً هناك من يقومو قبل تخزين الهاش باضافه نص اخر عليه Salt وبالتالي اذا حصل أن المخترق وصل لقاعدة البيانات فحتى لو كان المستخدم باسورده هو 1233 والذي يسهل استرجاع النص الأصلي من الهاش المخزن فسوف يصعب على المخترق بسبب أن ال saltاضيف لذلك الباسورد وبالتالي اذا كان ال saltصعب ايضاً فقد لا يتم ايجاد النص الأصلي لكلمة المرور السهله هذه، ولكن في النهايه ال salt يجب ان يخزن في مكان ما ، سواء في القاعدة أو داخل الكود أو في مكان ما المهم ان يكون الكود قادراً على استرجاعه بسهولة وبسرعه ، ربما بعض ال Obufscationيصعب على المخترق في هذا الأمر

آمل أن تكون المقالة الصغيرة قد افادتك وبينت لك فوائد الHashing ، ولو لاحظت أن تطبيقاتها كثيرة خصوصاً في مجال التحقيق الجنائي forensics وفي البحث عن البيانات، فيمكنك بسهولة الان القيام ببضعه تطبيقات صغيرة والتي عرضنا افكارها في المقالة

2-2 معيار تشفير البيانات DES

معيار تشفير البيانات (بالإنجليزية Data Encryption Standard :ويشار لها بالإختصار (DES هي خوارزمية مفتاح متناظر ساد لفترة ماضية لتشفير البيانات الإلكترونية. كان لها تأثير كبير في النهوض باساليب التشفير الحديثة في العالم الأكاديمي. وضعت في وقت مبكر من سبعينات القرن العشرين في شركة آي بي إم وصممت على أساس تصميم سابق من قبل هورست فستل Horst Feistel، قدمت الخوارزمية للمكتب الوطني للمعايير بعد دعوة الوكالة لاقتراح مرشح لحماية بيانات الحكومة الالكترونية الحساسة وغير المصنفة. في سنة 1976، بعد التشاور مع وكالة الأمن القومي ، اختارت مؤسسة الدولة للاحصاء في نهاية المطاف صيغة معدلة بشكل طفيف، والتي نشرت بوصفها معالجة المعلومات الاتحادية القياسية FIPSالرسمية للولايات المتحدة في عام 1977. أدى نشر اعتماد وكالة الأمن القومي الأمريكية لمعيار التشفير القياسي في تقريرها تزامنا لاعتماد دولي سريع وتدقيق أكاديمي على نطاق واسع. صنفت الخوارزمة أيضا في المعهد القومي الأمريكي للقياس بالرمز,X3.92 [6]

نشأت الخلافات حول عناصر سرية التصميم، طول المفتاح القصير نسبيا، تصميم شفرات كتلة متماثل ، وإشراك وكالة الأمن القومي، مغذية الشكوك حول باباً خلفية (backdoor)مستترة. التدقيق الأكاديمي المكثف للخوارزمية لأكثر من مرة أدى إلى الفهم الحديث لتشفير الكتلة وتحليل الشفرات الخاصة به.

وقد نشر هجوم نظري ،وفق تحليل الشفرات الخطية، في عام 1994، لكن هجوم القوة الغاشمة هجوم القوة العمياء في عام 1998 أظهر أن DES يمكن مهاجمته عمليا ، وسلط الضوء على الحاجة إلى استبدال الخوارزمية. هذه وغيرها من أساليب تحليل الشفرات تحليل الشفرات يتم مناقشتها بمزيد من التفصيل لاحقا في هذه المقالة.

يعد معيار التشفير القياسي الآن غير آمن للعديد من التطبيقات. أساسا بسبب حجم المفتاح (56 بت) الذي يعد الآن صغيرا جدا، ففي يناير 1999، تعاونت مؤسسة distributed.net ومؤسسة الحدود الإلكترونية علنا لكسر مفتاح (DES) في (22 ساعة) و (15 دقيقة). وهناك أيضا بعض النتائج التحليلية التي تبين نقاط الضعف النظرية في الشفرة، على الرغم من أنها غير مجدية في الهجوم في الممارسة العملية.يعتقد أن الخوارزمية تكون آمنة من الناحية العملية في شكلها الثلاثي DES3، وإن كانت هناك هجمات نظرية. في السنوات الأخيرة تم سحب DES كمعيار من قبل المعهد الوطني للمعايير والتكنولوجيا المعهد الوطني للمعايير والتقنية(سابقا المكتب الوطني

للمعايير). بعد أن تم كسر هذا التشفير في عام 2008م وتم استبداله بمعيار التشفير المطور (Advanced Encryption Standard)ويشار لها بالإختصار (AES) في أغلب الإستخدامات.

معيار تشفير البيانات عبارة عن خوارزمية لتشفير كتل من البيانات باستخدام المفتاح المتناظر،وهو كود تشفير بطول (64 بت) ولكن يستخدم منه (56 بت) فقط لعملية التشفير، وتستخدم (8 بتات) -وهي أول بت من أقصى يمين كل بايت- لتدقيق الأخطاء.وهي تأخذ كتلة بحجم (64 بت) من النص الأصلي وتخرج نص مشفر بحجم (64 بت). وتعتمد في عملها على عملية التعويض (substitution) والتبديل في الأماكن.(permutation)وتحتوي الخوارزمية على 16 دورة تتكرر فيها عملية التعويض والتبديل بين الأماكن حتى تنتج النص المشفر النهائي.

بعض الوثائق يميز بين DES كمعيار وDES كخوارزمية، مشيرا للخوارزمية (DEA) (خوارزمية تشفير البيانات).

Permutation 2-3

وهيه عدد التشكيلات الممكنة لمجموعة جزئية من العناصر منتقاة من مجموعة كلية من العناصر مع مراعاة لأهمية تسلسل العناصر في تشكيلات المجموعة الجزئية.

الفصل الثالث

3.1 نبذة عن لغة Html(html Language):-

HTMLهي اختصار لجملة **H**yper**T**ext **M**arkup **L**anguage، وهي لغة وشفرات برمجية يتم كتابتها يدوياً أو عن طريق برامج متخصصة ، ومن ثم يتم ترجمة هذه الأكواد والشفرات عن طريق متصفحات الانترنت (مثل انترنت اكسبلورر وفايرفوكس وغيرها) وتحويلها إلى صفحات انترنت منسقة ومرتبة على حسب اختيار ورغبة مصمِّم الصفحة وهي غير مرتبطة بنظام التشغيل.

يتم كتابة شفرات وأكواد هذه اللغة بإحدى الطريقتين التالية: -

1- WYSIWYG: -

هي اختصار لـ What You See Is What You Getومعناها ماتشاهده هو ماستحصل عليه. وهي عبارة عن استخدام برامج متخصصة في كتابة هذه اللغة (مثل فرونت بيج ومحرر النصوص وورد و دريم ويفر وغيرها (لتقوم بعمل صفحة انترنت بدون الحاجة لمعرفة وكتابة الشفرات البرمجية الخاصة بهذه اللغة، بمعنى أنه إذا أردنا مثلاً أن نكتب كلمة بلون معين ، كل ماعلينا هو كتابة الكلمة ثم نقوم بتظليلها في البرنامج ومن ثم نذهب إلى قائمة الألوان لنختار اللون الذي نريده، وهكذا لباقي عمليات التنسيق المختلفة، والبرنامج سيقوم بالنيابة عنا بتحويل ماعملناه إلى أكواد وشفرات HTML.
برنامج مايكروسوفت وورد هو أوضح مثال على مثل هذه البرامج ، حيث يمكننا عن طريقه عمل صفحة انترنت بالتنسيق الذي نريده – وكأننا ننسق مستند نصي عادي – وبعدها نقوم بحفظ الملف على شكل صفحة ويب ، وسنجد الملف الناتج يحمل امتداد html وهو الامتداد الخاص بصفحات الانترنت التي نستطيع فتحها ومشاهدتها بواسطة المتصفح.

يفضل استعمال هذا النوع لغير المحترفين في مجال عمل صفحات الانترنت أو لمن لايريد تعلمها لأنها ليست على علاقة مع تخصصه أو مجال عمله. ويميز هذا النوع بأنه يسمح لنا برؤية عملنا مباشرة في البرنامج، وأيضاً لايتطلب معرفة شفرات اللغة البرمجية.

2- Explicit Markup: -

هذه هي الطريقة الأساسية لكتابة هذه اللغة، وهي عبارة عن كتابة كل شفرة وكل حرف يتعلق بصفحة الانترنت المراد عملها ابتداءً من الصفر ونهاية بحفظ الصفحة ورؤيتها عن طريق متصفحات الانترنت ومن ثم التعديل على الشفرات إن كان ذلك لازماً.

هذه الطريقة هي التي سنستعملها بالطبع في شرحنا لهذه اللغة لأن الأخرى لاتحتاج إلى شرح ولايوجد فيها شفرات أو شيء يصعب على الناس فهمه.

يتم كتابة الشفرات عن طريق عدة برامج وأشهرها وأبسطها برنامج Notepad أو محرر النصوص العادي في الويندوز ، وبرنامج TextEdit في الماكنتوش ، نفتح ملف جديد ونكتب الشفرات والأكواد البرمجية فيه ، ومن ثم نعمل حفظ الملف باسم ، ونضع أي اسم نريده بشرط أن يحتوي على امتداد .html حتى نستطيع رؤية ماقمنا بعمله بواسطة متصفح الانترنت.

ميزة هذا النوع بأنه يسمح لنا بالتحكم بشكل أكبر في التصميم من الطريقة الأخرى، لأن بعض البرامج لاتوفر لنا بعض الخصائص أو الأوامر المتقدمة أو الغير مشهورة، وعيبه هو أن رؤية النتيجة تحتاج لعدة خطوات (حفظ الملف ثم فتحه بمتصفح انترنت) على عكس الطريقة الأولى.

3.2 مميزات هذه اللغة:-

- هي لغة بسيطة وسهلة غير مرتبطة بنظام تشغيل ، تستطيع استخدامها على لينوكس او ويندوز او ماك او اي نظام تشغيل في العالم
- لا يوجد قيود بهذه اللغة لأنها بسيطة
- ستطيع ادراج صور ونصوص وفيديو
- بإمكانك الاطلاع على كود HTML لاي صفحة على شبكة الانترنت مما يزيد من خبرتك بهذه اللغة.

3.3 لغة PHP

لغة البرمجة PHPعبارة عن لغة قوية جدا تستخدم لبرمجة وتطوير مواقع الانترنت الديناميكية والتفاعلية بقوة وصرامة وروعة في الأداء. وتعتبر هذه اللغة الأكثر شيوعا واستخداما في العالم. كما أنها تعد البديل المنافس للغات تطوير المواقع مثل Microsoft ASP.NET وغيرها.

تعتبر اللغة المناسبة لتطوير مواقع الانترنت حيث يمكن كتابة الكود الخاص بها بين وسوم لغة HTMLوتكون متداخلة معها بدون أي مشاكل.

مما يزيد من روعة هذه اللغة وقربها للمبرمجين أن الكود الخاص بها قريب جدا من كتابة كود لغات أخرى متل C و . PERLومن الجدير بذكره انها لغة مفتوحة المصدر مجانية الاستخدام وتستخدم عادة مع سيرفر Apacheاللذان يعملان سويا على كافة أنظمة التشغيل علاوة على ذلك فانه يمكن للغة PHPالعمل على IISالخاص ب Microsoftوعلى نظام التشغيل ويندوز .

بدايـــــة :

تعتبر لغة البرمجة PHP من اللغات المتطورة جدا كما ذكرت سابقا وللتذكير لبداية تعلم البرمجة باستخدامها يجب معرفة HTML اولا.... او لا تكمل من الدروس معنا

تعتبر MySQL هي عبارة عن قواعد البيانات المستخدم مع PHP وذلك لعدة اسباب أهمها السرعة والخفة والحفاظ على البيانات.

<u>بداية العمل مع PHP :</u>

لتبدأ البرمجة وتطبيق الدروس باستخدام لغة PHP تحتاج لتثبيت البرامج التالية :

1-سيرفر الاباتشي apache server والذي يمكن تحميله لويندوز أو لينكس بدون أي مشاكل

2-تنزيل لغة ال PHP

3-تنزيل قواعد البيانات MySQL

لو ذهبت الى أي صفحة مكتوبة بلغة PHP وذهبت الى عرض لكود المصدري فانك لن تجد أي حرف مكتوب بلغة PHP وكل ما ستجده هو وسوم HTML البعض يستغرب ويسأل عن السبب

السبب في هذا هو ان ال PHP من اللغات التي يتم تطبيقها على السيرفر وارسال النتائج الى المتصفح الذي بدوره يعرض وسوم HTML .

قبل كتابة الكود يجب أن يوجد الكود داخل صفحة بالامتداد php .

طريقة كتابة كود PHP :

كود PHP هو عبارة عن كود يبدأ ب php ؟> وينتهي ب ؟>. كما يمكن أن يتواجد في أي مكان داخل الملف بناء على الحاجة لوجوده.

<؟ php

؟>

ملف ال PHP هو عبارة عن ملف يحتوي عادة على اكواد PHP مدموجة مع وسوم HTML ويمكن من خلال الكود التالي فهم ما أقصده:

<؟ php

World echo "Hello "؛

؟>

كل أمر في كود لغة ال PHP يجب أن ينتهي بالفاصلة المنقوطة حيث تستخدم للفصل والتمييز بين الاوامر وبعضها البعض.

طبعا انتهينا من طريقة كتابة الكود الان وسأعود بعد الانتهاء من عمل اعمله لكيفية تعريف المتغيرات

المتغيرات في لغة البرمجة PHP

سنقوم اليوم بمعرفة طريق تعريف المتغيرات وكيفية استخدامها والتعامل معها .

لا يخفى على أحد مل للمتغيرات من أهمية في أي كود برمجي... حيث لا يخلو كود برمجي من متغير يتم استخدامه اما لتخزين قيمة أو رقم أو نص أو لاسترجاع قيمة من دالة أو غيرها وغيرها الكثير. لذا من الواجب معرفة كيفية تعريف المتغيرات والتعامل معها .

عندما تقوم بتحديد متغير فانه يمكنك استخدامه مرات عديدة داخل الملف .

لتعريف أي متغير في لغة البرمجة PHP يجب أن يبدأ اسم المتغير بعلامة الدولار $ ....يجب تذكر هذا جيداً

الطريقة الصحيحة لتعريف المتغير هي كالتالي :

كود PHP:

```
$variable_name = value ;
```

المبرمجون المبتدؤن في لغة البرمجة PHP عادة ما ينسون علامة الدولار في بداية تعريف المتغير. في هذه الحالة فان المتغير سيتعبر غير موجود لذا يرجى الانتباه .
الان سنقوم بتعريف متغيرين أحدهما يمثل نص والآخر يمثل رقم وأرجو ملاحظة الفرق :

كود PHP:

```
<?php

$txt = "Hello World!" ;

$number = 16

?>
```

لغة البرمجة PHP لا تحتاج لتعريف نوع المتغير حيث يمكنك تعريف المتغير أينما شئت كما انك غير مجبر على تعريف نوعه. وكما رأينا في المثال السابق فقد قمنا بتعريف متغير دون تحديد نوعه .

تقوم لغة ال PHP بتحديد نوع المتغير بناء على البيانات الموجودة فيه تلقائيا بعكس لغات البرمجة الاخرى مثل الجافا حيث تكون مطالبا بتعريف نوع المتغير وتحديد قيمة ابتدائية له .

في ال PHP يتم تعريف المتغير ونوعه عندما يتم استخدامه لاول مرة .

قواعد تعريف أسماء المتغيرات :

- اسم المتغير يجب أن يبدأ بحرف أو بالشرطة السفلية "_".

- اسم المتغير يمكن أن يحتوي فقط على حروف وأرقام والشرطة السفلية ولا استخدام للرموز الخاصة .

- لا يمكن أن يحتوي اسم المتغير على مسافات اطلاقا .

السلاسل الرمزية في PHP: String

يتم استخدام تعريف السلاسل الرمزية للمتغيرات التي تحتوي على أحرف أو رموز خاصة أخرى.
من خلال هذا الدرس سنقوم بتعريف أكثر الدوال استخداما في التعامل مع السلاسل الرمزية في لغة PHP.

بعدما أنشأنا متغيراً سنقوم الآن بتعريف كيفية التعامل معه حيث يمكن التعامل معه مباشرة أو من خلال دالة .

في المثال التالي سيتم تعيين Hello World جملة وتخزينها في متغير $txt

كود PHP:

```
<?php
$txt = "Hello World" ;
echo  $txt ;
?>
```

سيكون ناتج تنفيذ الكود السابق هو كالتالي :

Hello World

الربط بين سلسلتين رمزيتين :

قد نحتاج في بعض الأحيان لعرض سلسلتين رمزيتين كأنهما سلسلة واحدة ولهذا وجب وجود الربط بينهما ويتم ذلك كما في المثال التالي :

كود PHP:

```
<?php

$txt1 = "Hello World" ;

$txt2 = "1234" ;

echo $txt1 . " " . $txt2 ; ?>
```

وسيكون ناتج التنفيذ كالتالي :

Hello World 1234

اذا نظرنا الى الكود السابق ونتيجته سنجد اننا استخدمنا النقطة للربط بين متغيرين ووضعنا باستخدام علامات التنصيص مسافة بينهما. وهذه هي نبذة مختصره عن لغة php

3.4 نبذة مختصرة عن MySQL

تعتبر لغه MySQL اشهر نظام قواعد البيانات مفتوح المصدر

ماهي لغه MySQL ؟

ان MySQL لغه خاصه بقواعد البيانات

تخزن البيانات في MySQL في كائنات قواعد البيانات تسمى جداول .

ان الجداول هو عبارة عن مجموعه من البيانات المدخله والمتصله كما يتألف الجداول من اعمدة وصفوف.

تعتبر قواعد البيانات مفيده جدا عند تخزين المعلومات بشكل تصنيفي اي عند استخدام شركه لقواعد البيانات يمكن ان تستخدم الجداول التاليه :

"Employees" و "Products" و "Customers" و "Orders"

جداول قواعد البيانات

تحتوي غالبا قواعد البيانات على جدول البيانات على جدول او اكثر يتم تعريف كل جدول باسم (Customers او Orders) .

كما يحتوي الجول على صفوف واعمده بالاضافه الى البيانات.

الاوامر Queries

الاوامر هي عباره عن طلبات او اسئله .

باستخدام MySQL يمكن تقديم اوامر لقواعد البيانات معلومات معينه والتي تحتوي على امكانيه تقديم النتائج من خلال الصفوف والاعمده

لاحظ الامر التالي:

SELECT LastName FROM Persons

يختار الامر السابق جميع البيانات الموجوده في عمود الكنيه LastName من الجدول المسمى Persons.

حقائق حول قواعد البيانات MySQL

احد الحقائق المهمة عن MySQL انها تقوم بتخزين البيانات الضمنيه الموجوده في التطبيقات وهذه حقيقه مذهله بسبب انت بعض الناس تعتقد ان MySQL تستخدم فقط مع التطبيقات التي تخزن البيانات صغيرة او متوسطه .

لكن الحقيقه بأن MySQL تستخدم مع القواعد البيانات مع مواقع الانترنيت التي تستخدم لتخزين هائل للبيانات والمستخدمين مثل Friendster و Yahoo و Google.

الفصل الرابع

الجانب العملي

4.1 واجهة النظام الرئيسية

من خلال الواجهة النظام الرئيسية يمكن تشفير وايضا البحث عن طريق الشفرة وايضا عرض الشفرات والكلمات التابعة للشفره في جدول اسفل فورمة الادخالات كما موضح في الجدول اعلاه.

4.2 جدول قاعدة بيانات النظام

يتم خزن شفرات md5 داخل هذا الجدول حيث يمكن استدعائها في اي وقت وايضا البحث عنها

4.3 خوارزمية التشفير

```php
<?php
include 'c.php';
if($_GET['str']){
$string = $_GET['str'];


$sha1pass = md5($string);

$dbadduser = mysql_query("INSERT INTO md5
(combination,md5)
VALUES
('$string','$sha1pass')
"
)
or die(mysql_error());


}
?>
```

المصادر

---

[1] كتاب خواريزم تشفير البيانات بـ md5 المؤلف : حسين احمد طالب السنة : 2013

[2] كتاب حماية موقعك من السرقة بإستخدام Md5 وتشفير المستخدمين بمكتبه Md5

المؤلف : الزهيري السنة : 2009

[3] كتاب PHP-basics المؤلف : محمد هاني لقموش السنة :2014

[4] كتاب التصميم بـhtml المؤلف : علاء الدين الجرادي السنة 2010

[5] تصميم قواعد البيانات تأليف : المؤسسة العامة للتعليم الفني والتدريب المهني السنة : 2008

[6] ISO/IEC 18033-3:2010 Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers". Iso.org. 2010-12-14