



جاهز. الآمن الاتصال أن لتأكيّد الجلّسة بمفتاح مشفرة  رسالة الجوانب كلتا يرسل

مما الجلّسة، بمفتاح الملفات  أو الاستمارات، الويب، صفحات  مثل البيانات جميع تشفير يتم،  إتمام بعد يسرقها. قد شخص لأي للقراءة قابلية غير يجعّله

تعمل؟ وكيف  شهادات هي ما

معرفته: إلى تحتاج ما إليك التشفير. وتتيح الويب موقع هوية تثبت رقمية وثيقة هي  شهادة

. الشهادات مركز من رقمية ووقعة العام، ومفتاحه الموقع، نطاق اسم على الشهادة تحتوي: المحتوى

العام المفتاح وتوفر مزيّف  موقع إلى وليس example.com إلى بالفعل تربط أنك  مثل شرعي الخادم أن تضمن: الغرض  للتشفير.

المتصفح: يفتش: التحقق

1. ملغاة؟ أو من تهية  غير صالحة الشهادة هل

2.  مثل الموثوقة الشهادات مراكز من مدمجة قائمة على المتصفحات  يحتوي به؟ موثوق شهادات مركز وقعتها هل .  أو

ويواصل بالخادم المتصفح يثق الفحوصات، مرت إذا .

ويسرقوا موقع أي بأنهم يتظاهروا أن للمهاجمين يمكن ذلك، بدون الموقع. هوية يضمن به موثوق ثالث لطرف الشهادات مركز يعمّل بياناتك.

التشفير من الغرض

المتجانس التشفير و المتجانس غير التشفير من مزيج إلى  في التشفير يستند

1.  خلال المتجانس غير التشفير:

سرّاً. الخادم به  يحتفظ سرّيّ مفتاحاً وعلناً  مشاركة عامّاً مفتاحاً يستخدم

يفسره. أن يمكن السري، بمفتاحه الخادم، فقط العام. الخادم بمفتاح   المتصفح يشفّر

الإلهيلجية بالامن حنيات التشفير أو  الألغوريثم: على أمثلة .

2. للجلّسة:  المتجانس التشفير

البيانات. وتشفير لتشفير الجلّسة مفتاح الجوانب كلتا يستخدم الجلّسة، مفتاح إنشاء بعد

الكبيرة. البيانات لنقل مثاليّا ويجعّله المتجانس غير التشفير من أسرع هذا

الإلهيلجية بالامن حنيات التشفير أو  الألغوريثم: على أمثلة .

العمل المتجانس التشفير يتولى ثم آمن، بشكل الجلّسة مفتاح لنقل المتجانس غير التشفير  يستخدم الكفاءة. أجل من

### 1.3 و 1.2 بين أفرق

الرئيسية: أفرق إلك والحقن. الجديد إصدار هو 1.3 حيث، بروتوكول من إصدارات 1.3 و 1.2

الميزة	1.2	1.3
سرعة	يضيف مما والخدام، العميل بين رحلات عدة تأخير.	الأسرع. للاتصالات واحدة، غالبًا رحلات، أقل عند هـ فورًا البيانات إرسال يمكن إعادة الاتصال.
	أما الأقل القديم، التشفير ألغوريثم يدعم 1.0 مثل.	فقط يستخدم القديم، ألغوريثم يبعد مثل والأمني الحديث ألغوريثم.
الخصوصية	مثل هـ بيانات بعض عادي. نص في إرسالها يتم الشهادات 0	من المزيد تخفي مشفرة، هـ معظم المستمعين. عن التفاصيل إعادة عند فورًا البيانات إرسال يسمح إذا المتكررة الهجمات خطر هناك ولكن الاتصال، صحيح. بشركت أميها يتم لم
الأمان	الميزات بسبب الهجمات لبعض عرضة القديم.	الخيارات يبعد التصميم، من أقوى الضعيفة.

الحديث. لل معيار يجعله 1.2، من خصوصية أكثر و أمان و أسرع 1.3 الاختتام، في

### شيء لكل جمع

على الاعتماد 2. مشفر. اتصال لإنشاء هـ استخدام 1. خلال: من الإنترنت عبر التواصل أمان هـ من و هـ المتجانس غير التشفير استخدام 3. الخدام. هوية لتأكيد الموثوقية الشهادات مراكز من هـ على تحسن التي، 1.3 مثل بروتوكولات مع التطور 4. بياناتك. لحماية البيانات هـ لنقل المتجانس التشفير والخصوصية. والأمان السرعة خلال من 1.2

جزء. أي في عميق غوص في ترغب كنت إذا أخبرني تصفحك! لحماية هـ عمل كافي جودر هو هذا