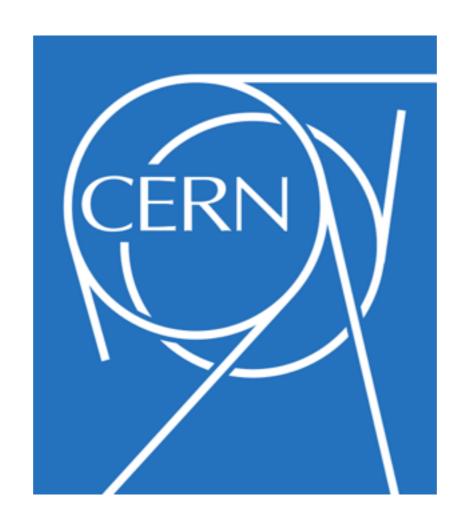
Using Let's Later Later

Optimizing TLS

HTTP



HTTPS



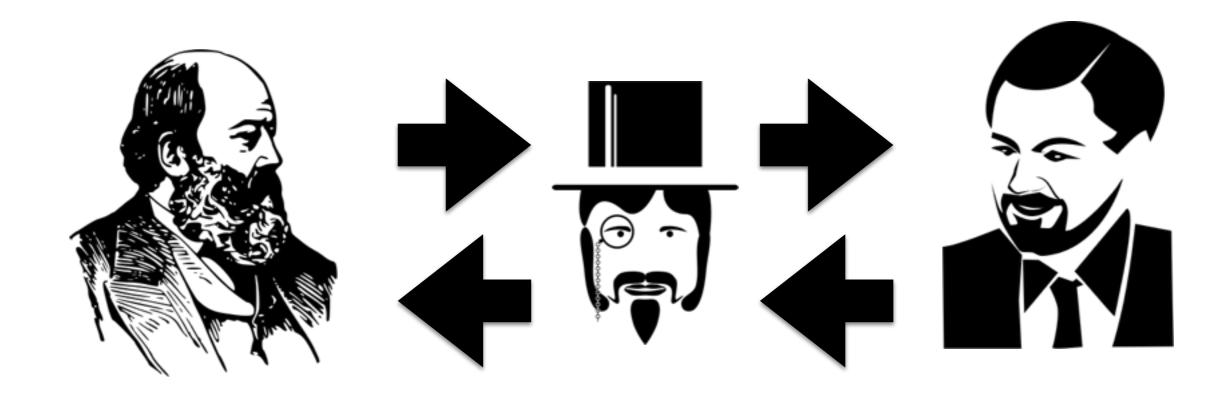
E-commerce



Identity Theft



Man in the Middle



Observe and/or Manipulate Content

Content Injection



Mass Surveillance



HTTPS Barriers





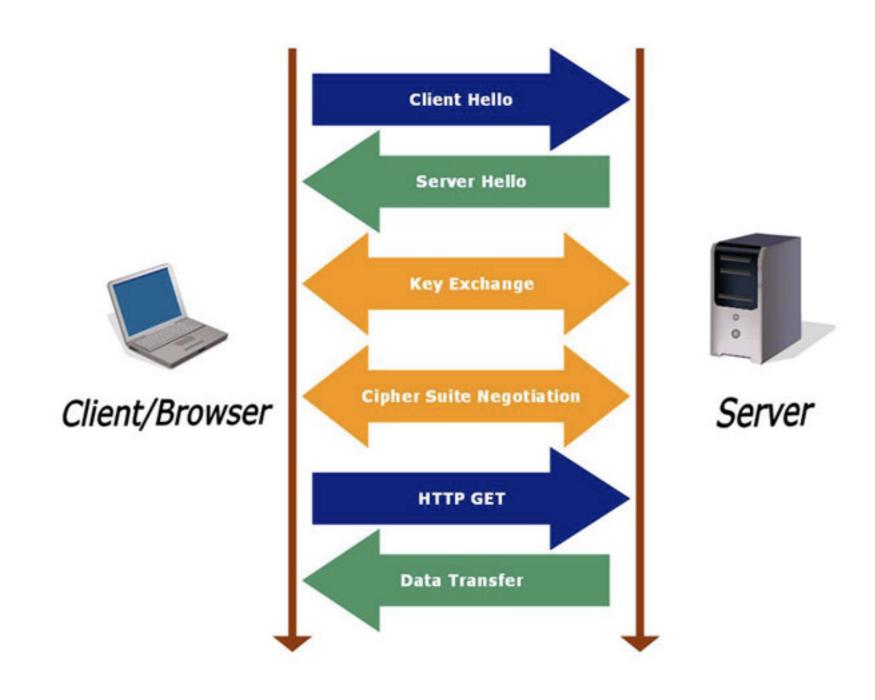


Cost

Technical

Motivation

SSL & TLS



RSA Private Key Size

Strong

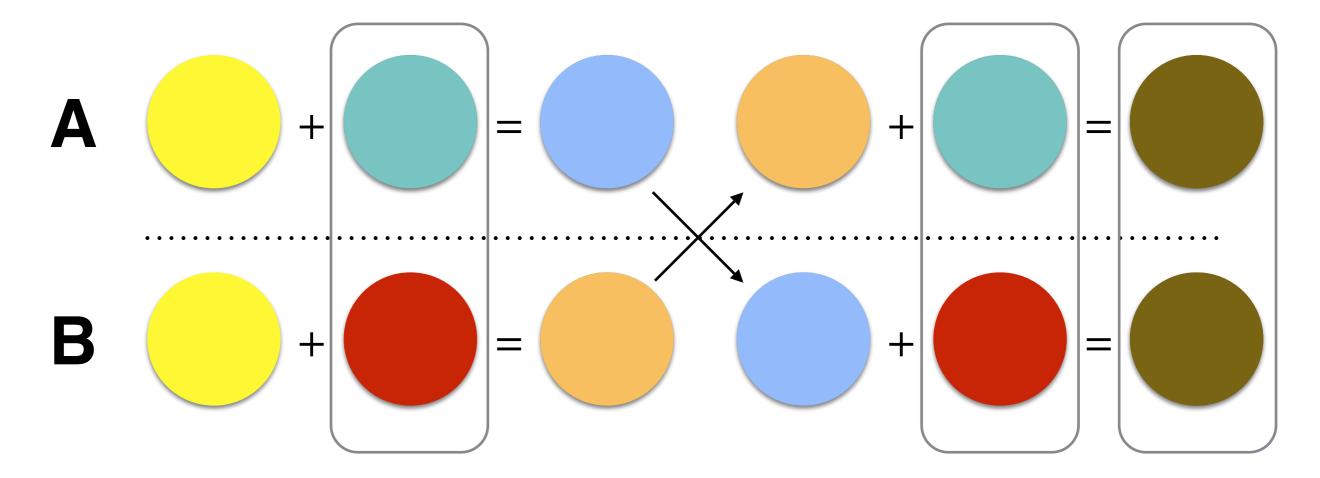
>= 2048

Weak

< 2048

Forward Secrecy

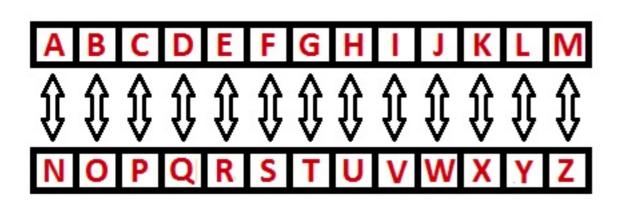
- DHE -Diffie-Hellman Ephemeral
- ECDHE Elliptic Curve Diffie-Hellman Ephemeral

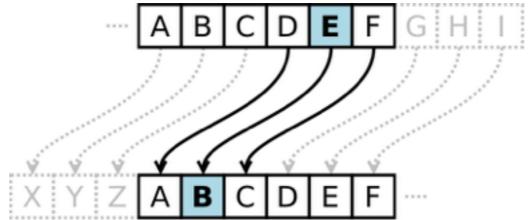


Confidentiality

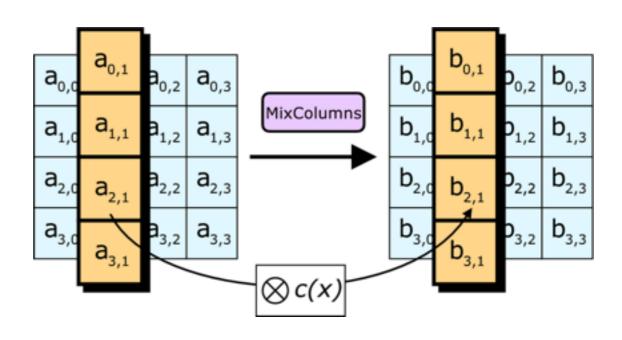


Cyphers









Cipher Strength

Strong AES 128/256

Weak

3DES

Broken

RC4

Recommended Ciphers

Block AES-GCM/CCM/CBC* ChaCha20-Poly1305* **Stream**

Integrity



Message Authentication Code

Strong

Weak

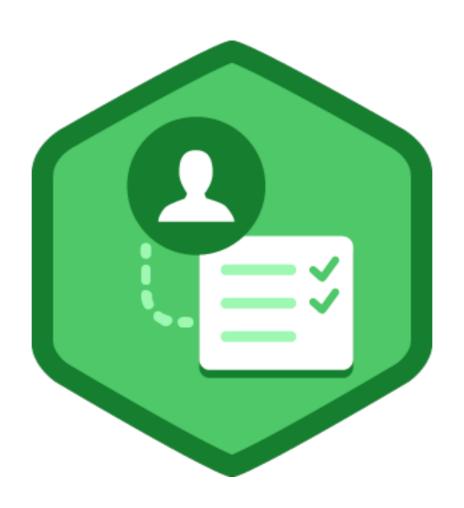
Broken

SHA-2+/ AEAD

SHA₁

MD5

Authenticity



Root Certificates

(Installed in your Browser)

---- BEGIN KEY ---

AAAAB 3II:va Ci yoʻZEAAAAAQAQBAAAA AQOVI pPI Digamik Misci Li yoʻganimle HU1880 Tingdalu X2R8AJ OJI rJA FOQUS OSOS SHIP ZBIP ZZYYYYI T3qi tuhkidi Kay I I pdAF-28 unX8Mduno AJIKFI ji XI IKXIL Cari La F85 400 ED milla Hispa I Xiriqimi huliv 1297 AVXI SIN CARI Viliqimi huliv 1297 AVXI SIN CARI HI YSOS YAYO XI YOʻZI YOʻXI YOʻZI YOʻX

2W1mHapeIXWqWm1wUviZqs
----- END KEY

---- BEGIN KEY

ADDV1.PT1pt.gmid.NNGC-17/Sp6n1Nt-1 413801Tpggall-12/Rbi/0.J17 JA-FRQX8 5085pHF26wFa2ZYVYI3qQtuMikG8 5085pHF26wFa2ZYVYI3qQtuMikG8 KAY1TpddAF28mXR8MidmaA, MiFhjEII TRRaxMaVv6yETAX35bkpaQVX2F5 XIXXdLCati. a185840bcbaYMIAHape XWkplm1uVv1zQ574XQ1MLDCArHk; ETFAS780kxWTSoLqxDkrN6WG709 HHj FX56KYQdZYCyeUP8unXRMidma AJWFhjEIITRxaxMaVv6yETAX35bk

----- FND KFY --

---- BEGIN KEY ----

---- END KEY -

GoDaddy

Comodo

Symantec

DigiCert

Intermediate Certificates

(Signed by a Root Certificate)

---- BEGIN KEY ----

AAABSIN:acI.ycZEAAAAOAQBAAAC AQOVI.PpI:kgskiKK6cI.VpSnfMle +U1880:Tiggdalv2R8Ai.OJr.JA:r0X8 5065bWF2Bmy2ZYYYY13qcUtmo KayI.TpdAF-28unX8MdunoAJWFhjEI TrFazYMSWY5F4X35bkqa0f5 XIKXdCLoni.LaF8540bCbm2NimHape Dioqimi-huti-ygZ74XQINU.CAG HyPSSKYGXGY HYPSSKYGY HYPSSKYG

---- END KEY

---- BEGIN KEY ----

----- END KEY --

---- BEGIN KEY ---AAAAB3NzaC1yc2EAAAADAQABAAAC

----- END KEY -

---- BEGIN KEY ----

10M1.pT.jk.gmwk.HKSc1./Xp.6nHHE 1180-TIngdulx.2R.8wJ0.Jr.JArRQX8 1285.pHr.26wPa.2ZYUYYI3.qQt.uhWGB 14y1.tpd4.2ZYUYYI3.qQt.uhWGB 14y1.tpd4.72WJ5.hyg.2VJ5. 15XGLC.an.LaF85.40bC.mZVI.mHape (Moyllam Lut J.2g7.4XQI.NLO.CAL 11r.AS78.dc.HC.VSol.qxXbk.YSWC7.99 19XS.6XYQd.2Y.yc.yelP8unX8Ndumo NFF.HEITT.RaxMYMV5yET4X35bk

---- END KEY

GoDaddy

Comodo

Symantec

DigiCert

Website Certificates

(Signed by an Intermediate Certificate)

openwest.org

AAAABHIZ LI Y Z EAAAADAQABAAAC
QOV I PI JI K BIMKING LI Y Y JOGHNIE
GOOD THE STANDAY THE STANDAY THE STANDAY
BOOD THE STANDAY THE STAND

eff.org

DEUIN KE.

AAAB3HxaCycZEAAAAAA(ABAAACA
AQDV.pFlxgmwktkci.VgmmHE
ell860mfgadus/seko.J01/AroKgs
SQ65paftZebraZZYvirl13qdvuwk66
SQ65paftZebraZZYvirl13qdvuwk66
SQ65paftZebraZZYvirl13qdvuwk66
SQ65paftZebraZZYvirl13qdvuwk66
SQ65paftZebraZZYvirl13qdvuwk66
SQ65paftZebraZZYvirl13qdvuwk66
SQ65paftZebraZZYvirl13qdvuwk67
XIXxdCcn11af8540bcDraZyvirl1afape
XIXxdCcn1af8540bcDraZyvirl1afape
XIXxdCcn1af8540bcDraZyvirl1afape
SQ65paftZebraZyvirl1afape
SQ65paftZebraZyvirl1afa

dc801.org

Certificate Lifecycle



Certificate Authority



Generate Private Key



Generate CSR



Submit CSR to CA





Validate Request

Install Certificate



←



Generate Certificate

Provide Certificate

Configure Webserver



Types of Validation

Domain	Controls the Domain		
Organization	Prove Organization's Legal Entity		
Extended	Manual Verification of Organization		

Certificate Authorities



Monopoly



Cartel













Network Solutions.

Alternatives







Using



ACME

Automated Certificate Management Environment

- Prove to the CA that it controls one or more domains(s).
- Request, renew, and/or revoke certificates for the domain(s)

ACME Agents

- CertBot (Recommended EFF)
- Caddy (Easy & Feature Rich)
- ZeroSSL (Browser)
- ACME Tiny (< 200 lines of Python)
- Letsencrypt-plugin (Ruby on Rails)
- Certify (Windows)
- Acme-client (Java)

A more comprehensive list can be found at: https://github.com/certbot/certbot/wiki/Links

Certbot Installation

wget https://dl.eff.org/certbot-auto **WGET** chmod a+x certbot-auto Varies depending on operating system and web **Package** server

Plugins

Module	Authentication	Installation
apache	Yes	Yes
standalone	Yes	No
webroot	Yes	No
nginx	Yes	No

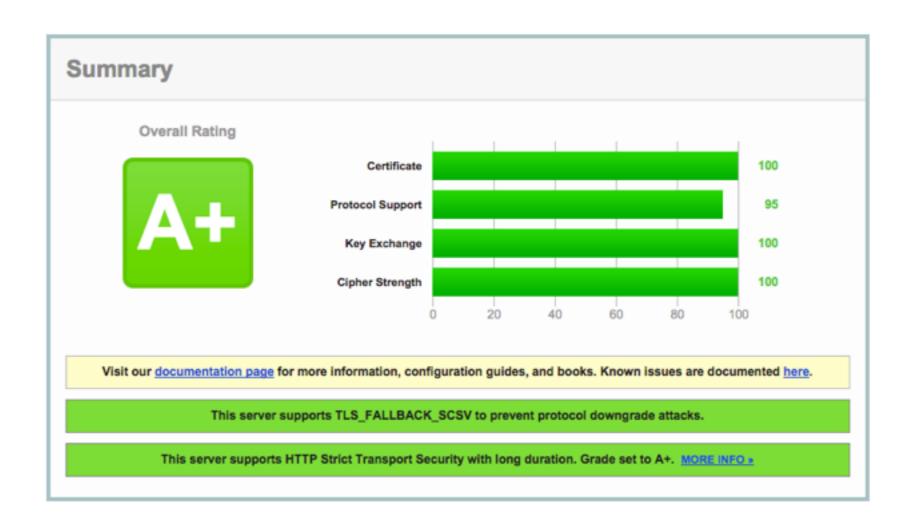
Examples

Basic/Apache	./certbot-auto		
Standalone	./certbot-auto certonlystandalone		
Webroot	./certbot-auto certonlywebroot		
Nginx	./certbot-auto certainly		
Renew	./certbot-auto renew		
Help	./certbot-auto help		

https://certbot.eff.org/docs/

Optimizing TILS

Making the Grade



https://ssllabs.com

Other Scanners

- HT Bridge https://www.htbridge.com/ssl
- nmap --script ssl-enum-ciphers -p 443 HOSTNAME
- openssl s_client -connect HOSTNAME:443 -prexit
 -showcerts -state -status -tlsextdebug -verify 10

Compatibility















Configuration



Mozilla SSL Configuration Generator



https://mozilla.github.io/server-side-tls/ssl-config-generator/

Nginx

```
server {
    listen *:80;
    return 301 https://$host$request_uri;
}
```

Nginx

Nginx

```
ssl_stapling on;
ssl_stapling_verify on;
add_header Strict-Transport-Security "max-age=31536000;
    includeSubdomains; preload";
add_header Public-Key-Pins
    'pin-sha256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=";
    pin-sha256="kl023nT2ehFDXCfx3eHTDRESMz3asj1mu0+4aIdjiuY=";
    max-age=518400';
```

Apache

```
<VirtualHost *:80>
          ReWriteEngine on
          ReWriteCond %{SERVER_PORT} !^443$
          ReWriteRule ^/(.*) https://%{HTTP_HOST}/$1 [NC,R,L]
</VirtualHost>
```

Apache

Apache

```
LoadModule headers_module modules/mod_headers.so

Header set Public-Key-Pins "pin-sha256=
\"kl023nT2ehFDXCfx3eHTDRESMz3asj1mu0+4aIdjiuY=\"; pin-sha256=
\"633lt352PKRXb0wf4xSEa1M517scpD3l5f79xMD9r9Q=\"; max-age=2592000;
includeSubDomains"

Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains"

</VirtualHost>
</IfModule>
```

IIS

IIS Crypto - 1.5 build 6					
Protocols Enabled Multi-Protocol Unified Hello PCT 1.0 SSL 2.0 SSL 3.0 ▼ TLS 1.0 ▼ TLS 1.1 ▼ TLS 1.2	Ophers Enabled NULL DES 56/56 RC2 40/128 RC2 128/128 RC4 40/128 RC4 56/128 RC4 56/128 RC4 128/128 RC4 128/128 V Triple DES 168/168 AES 256/256	Hashes Enabled MD5 SHA SHA 256 SHA 384 SHA 512	Key Exchanges Enabled ✓ Diffie-Hellman ✓ PKCS ✓ ECDH		
		to save your changes. Best Practices PCI	e a preset template. Click the Apply button EIPS 140-2 Defaults		
LH:			Şcan		
NARTAC SOFTWARE C	opyright © 2011-2014 Nartac Softwar	e Inc.	Apply		

https://www.nartac.com/Products/IISCrypto

Extra Credit

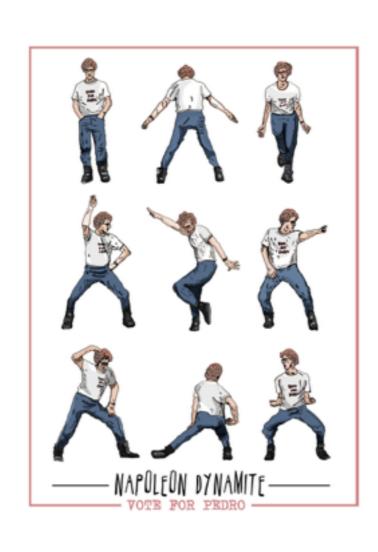
HTTP Strict Transport Security

HSTS Preloading https://hstspreload.appspot.com

OCSP Stapling

HTTP Public Key Pinning (HPKP)

Dance like no one is watching





Encrypt like everyone is