

SECURISER LE WEB AVEC HTTPS

MEETUP MARS 2019

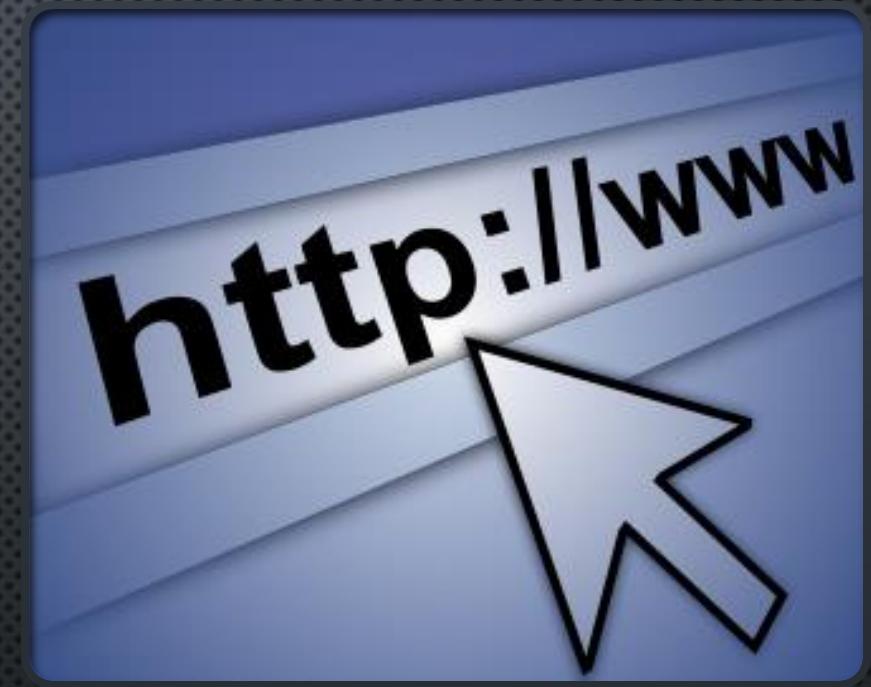
HTTPS: QU'EST- CE QUE C'EST ?

HTTP
+ SSL ou TLS

HTTPS

HTTP: ORIGINES

- HYPERTEXT TRANSFERT PROTOCOL
- PROTOCOLE APPLICATIF DE COMMUNICATION CLIENT-SERVEUR
- TIM BERNERS-LEE
- 1990s
- CENTRE EUROPÉEN POUR LA RECHERCHE NUCLÉAIRE
- WWW: HTTP, URL, HTML



HTTP: FONDATIONS

- HTTP UTILISE LE PROTOCOLE RÉSEAU TCP/IP (1970s)
- SUR LE RÉSEAU DE MACHINES " INTERNET " (1960s)
- PROTOCOLE SANS ETAT (CF. COOKIES, SESSIONS)



HTTP: LA REQUETE

COMMANDE (VERBE, URL, VERSION)
ENTÊTES
CORPS (PEUT ÊTRE VIDE)

GET /MAPAGE.HTML HTTP/1.1
HOST: WWW.EXAMPLE.COM
(VIDE)

VERBES: GET, POST, PUT, PATCH, DELETE,
HEAD, OPTIONS, TRACE, CONNECT



HTTP: LA RÉPONSE

STATUT (VERSION, CODE, LIBELLE)
ENTÊTES
CORPS (PEUT ÊTRE VIDE)

HTTP/1.1 200 OK
CONTENT-TYPE: TEXT/HTML
<HTML>
 <BODY>
 <P>CONTENU DE LA PAGE<P>
 </BODY>
</HTML>

CODES: 2XX, 3XX, 4XX, 5XX



HTTP: EN CLAIR

- N'IMPORTE QUI ENTRE LE CLIENT ET LE SERVEUR PEUT ECOUTER LES ÉCHANGES
- ENCORE PLUS FACILE AVEC LE WI-FI (1999)
- QUID DU E-COMMERCE (1995) ?



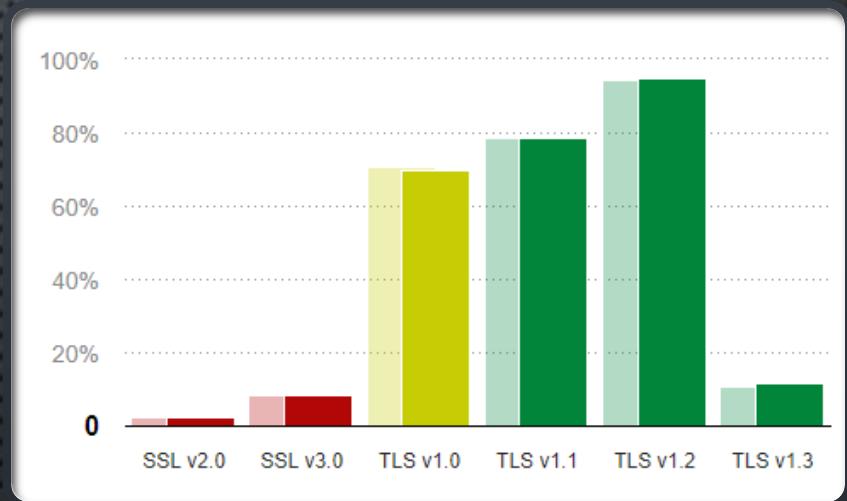
SSL

- SECURE SOCKETS LAYER
- PROTOCOLE DE SECURISATION DES ECHANGES (TRANSPORT)
- NAVIGATEUR NETSCAPE
- SSL 2.0 (1995)
- SSL 3.0 (1996)
- FAILLES DE SECURITÉ: SSL v2 ET v3 SONT BANNIS (2011 ET 2015)



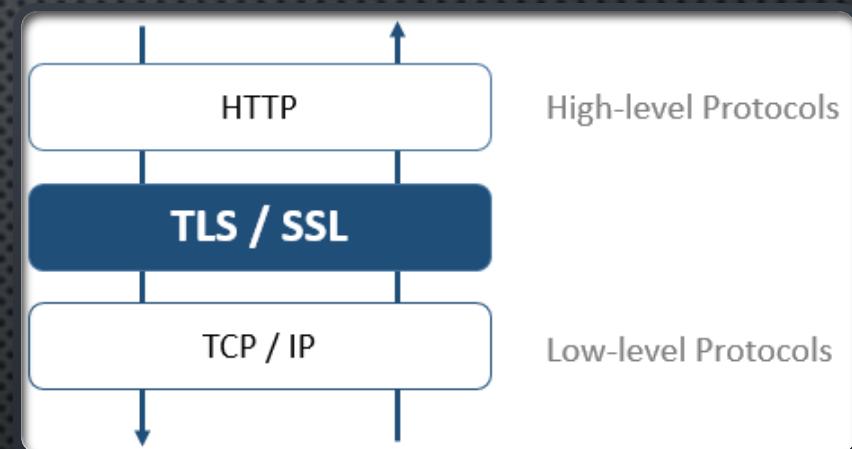
TLS

- TRANSPORT LAYER SECURITY
- INTERNET ENGINEERING TASK FORCE
- TLS 1.0 (1999)
- TLS 1.1 (2006)
- TLS 1.2 (2008)
- TLS 1.3 (2018)
- LA PLUPART DES NAVIGATEURS MODERNES GÈRENT TLS 1.1 ET 1.2
- TLS 1.0 ET 1.1 SERONT BANNIS EN 2020



TLS/SSL: FONCTIONNEMENT

- COMME SSL, TLS S'INTERCALE ENTRE TCP/IP ET HTTP
- DEUX SOUS-PROTOCOLES:
HANDSHAKE: AU DÉBUT DE LA SESSION
RECORD: POUR ECHANGER LES DONNEES



LES COUCHES DU MODÈLE OSI

1. COUCHE PHYSIQUE (HUB)
2. COUCHE LIAISON (TRANSFERT VERS LES NOEUDS ADJACENTS)
3. COUCHE RÉSEAU (ROUTER VERS LES VOISINS DIRECTS)
4. COUCHE TRANSPORT (COMMUNICATION DE BOUT EN BOUT)
5. COUCHE SESSION (TRANSACTIONS)
6. COUCHE PRÉSENTATION (DECODAGE)
7. COUCHE APPLICATION (DIALOGUE)



TLS/SSL: HANDSHAKE

- CHOIX DU PROTOCOLE (SSLv3, TLS1.0, TLS1.1, TLS1.2 ?)
- CHOIX DU CHIFFREMENT SYMETRIQUE (PARMI CEUX EN COMMUN)
- AUTHENTIFICATION (CERTIFICATS)
- ECHANGE DES CLES



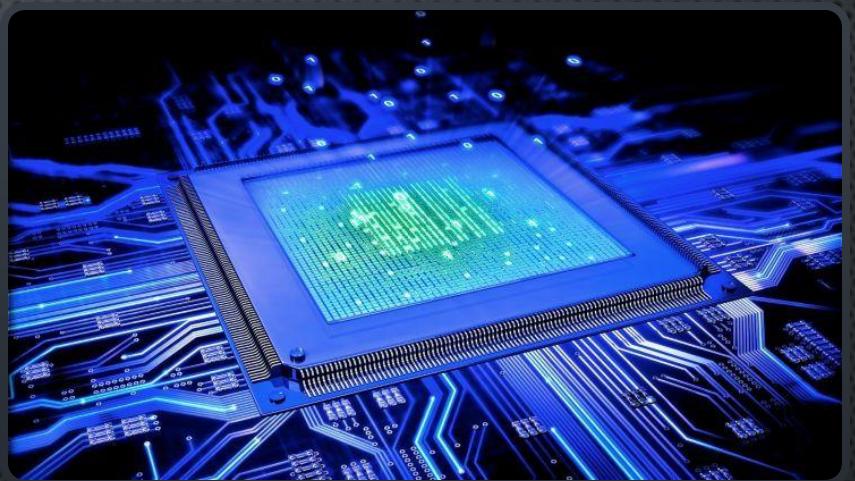
CHIFFREMENT SYMETRIQUE ?

- CHIFFRER ET DECHIFFRER DES MESSAGES À L'AIDE D'UNE CLE SECRETE ET D'UN ALGORITHME (ENV. 2000 AV. JC)
- EXEMPLE AVEC LE CHIFFREMENT DE CÉSAR (ENV. 60 AV. JC):
PERMUTATION CIRCULAIRE DE L'ALPHABET (ALGORITHME)
DÉCALAGE DE +3 (CLÉ SECRETE)
- AVANTAGES: TRES FACILE À CHIFFRER/DECHIFFRER MANUELLEMENT AVEC LA CLÉ
- INCONVENIENTS: ECHANGE DE LA CLÉ PRÉALABLE, TRÈS FACILE À DECRYPTER SANS LA CLÉ (26 POSSIBILITÉS)



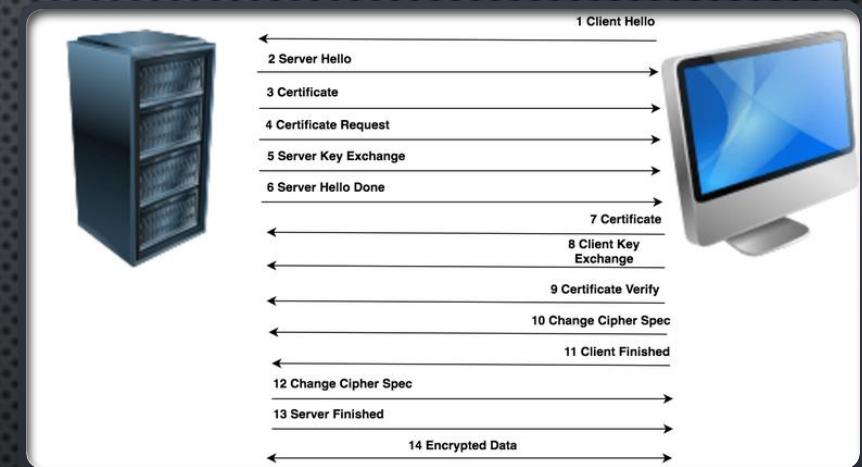
CHIFFREMENT SYMETRIQUE ?

- EXEMPLE AVEC LE CHIFFREMENT AES128 (ENV. 2000 AP. JC):
RIJNDAEL (ALGORITHME)
128 BITS (CLÉ SECRETE)
- LA SECURITÉ REPOSE ENTIÈREMENT SUR LA CLÉ (128, 192 OU 256BITS)
CAR L'ALGORITHME EST CONNU (PAS DE SECURITÉ PAR L'OBSCURITÉ)
- AVANTAGES: TRES TRES FACILE À CHIFFRER/DECHIFFRER (2008 SUR x86) AVEC LA CLÉ
- INCONVENIENTS: ECHANGE DE LA CLÉ PRÉALABLE !!



TLS/SSL: HANDSHAKE

- COMMENT ECHANGER UNE CLE SYMETRIQUE SANS SE CONNAITRE AVANT NI L'ENVOYER EN CLAIR ??
- GRACE AU CHIFFREMENT ASYMETRIQUE



CHIFFREMENT ASYMETRIQUE ?

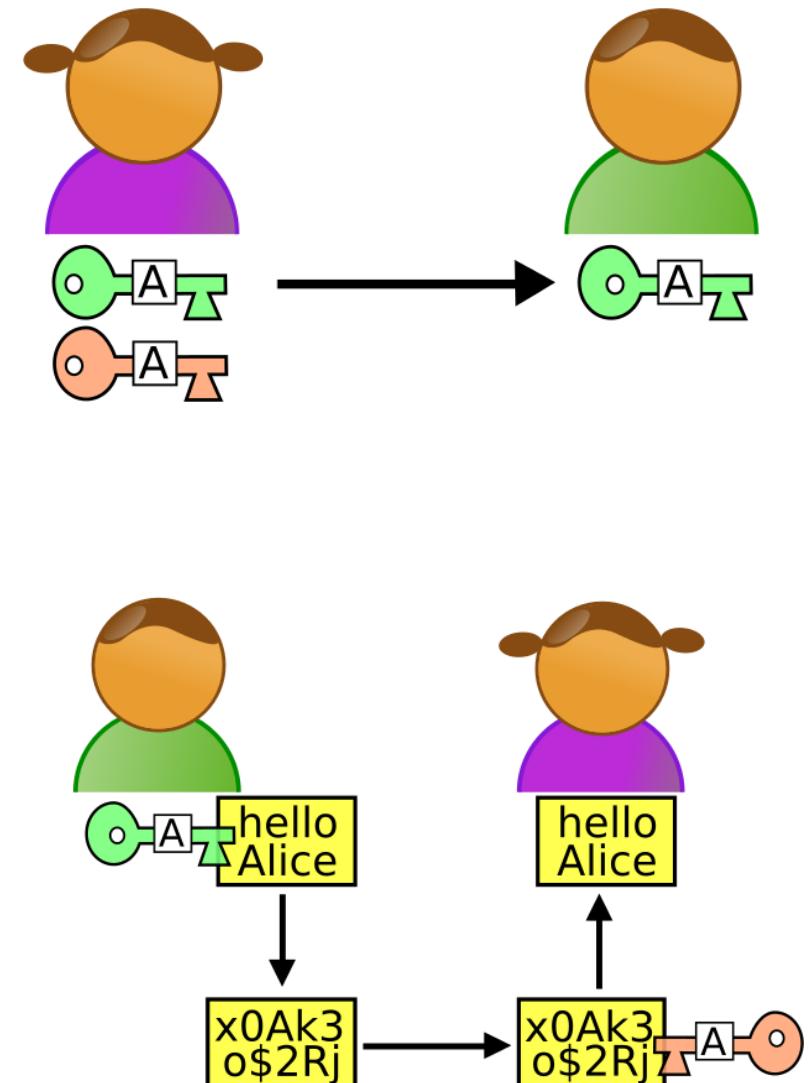
- CHIFFRER ET DECHIFFRER DES MESSAGES À L'AIDE DE CLÉS PUBLIQUES ET DE CLÉS PRIVÉES (PKI)
- LA CLÉ PUBLIQUE SERT À CHIFFRER ET À AUTHENTIFIER
- LA CLÉ PRIVÉE SERT À DÉCHIFFRER ET À SIGNER
- DEUX FAMILLES D'ALGORITHMES:
 - BASÉ SUR LES NOMBRES PREMIERS: RSA (1983), DSA (1993)
 - BASÉ SUR LES COURBES ELLYPTIQUES: ECDSA (1995), EDDSA (2011)



CHIFFREMENT ASYMETRIQUE: CHIFFRER/DECHIFFRER

1. ALICE GÉNÈRE DEUX CLEFS. LA CLEF PUBLIQUE (VERTE) QU'ELLE ENVOIE À BOB ET LA CLEF PRIVÉE (ROUGE) QU'ELLE CONSERVE PRÉCIEUSEMENT SANS LA DIVULGUER À QUICONQUE.
2. BOB CHIFFRE LE MESSAGE AVEC LA CLEF PUBLIQUE D'ALICE ET ENVOIE LE TEXTE CHIFFRÉ.
3. ALICE DÉCHIFFRE LE MESSAGE GRÂCE À SA CLEF PRIVÉE.

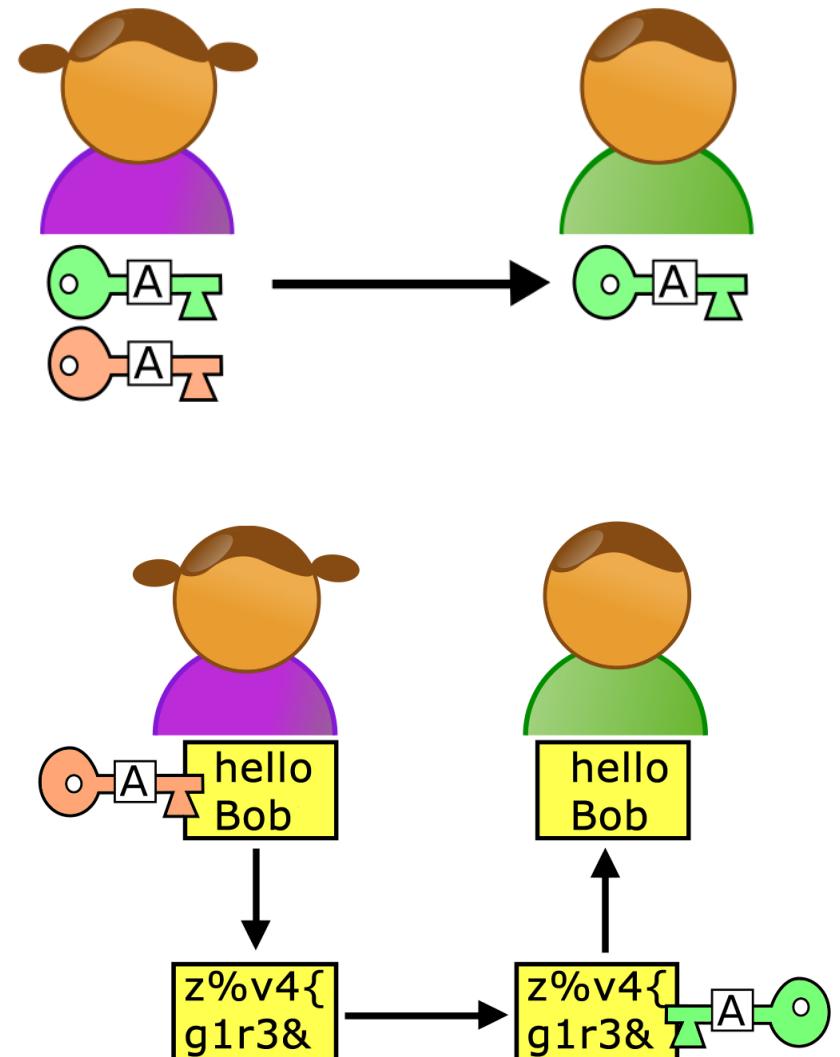
SEULE ALICE PEUT DÉCHIFFRER LE MESSAGE MAIS ON NE PEUT PAS GARANTIR QU'IL VIENT DE BOB.



CHIFFREMENT ASYMETRIQUE: SIGNER/AUTHENTIFIER

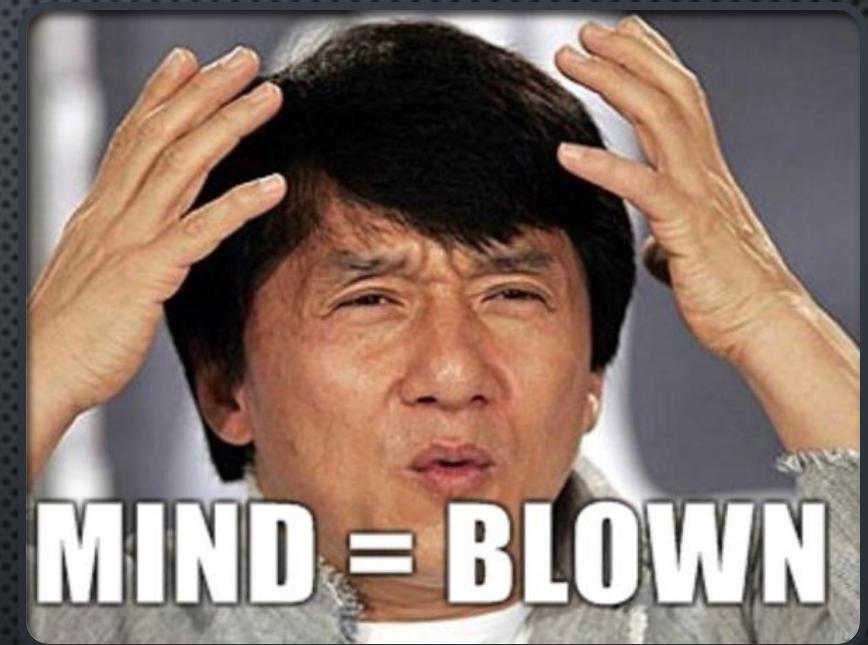
1. ALICE GÉNÈRE DEUX CLEFS. LA CLEF PUBLIQUE (VERTE) QU'ELLE ENVOIE À BOB ET LA CLEF PRIVÉE (ROUGE) QU'ELLE CONSERVE PRÉCIEUSEMENT SANS LA DIVULGUER À QUICONQUE.
2. ALICE CHIFFRE LE MESSAGE AVEC SA CLEF PRIVÉE ET ENVOIE LE TEXTE CHIFFRÉ.
3. BOB DÉCHIFFRE LE MESSAGE GRÂCE À LA CLEF PUBLIQUE D'ALICE.

TOUT LE MONDE PEUT DÉCHIFFRER LE MESSAGE MAIS IL EST GARANTI QU'IL VIENT D'ALICE.



CHIFFREMENT ASYMETRIQUE: CHIFFREMENT + AUTHENTICATION

1. ALICE ET BOB GÉNÈRENT CHACUN DEUX CLEFS. LA CLEF PUBLIQUE (V ERTE) ET LA CLEF PRIVÉE (ROUGE). ILS ECHANGENT LEUR CLE PUBLIQUE.
2. ALICE CHIFFRE LE MESSAGE AVEC SA CLE PRIVEE ET CHIFFRE LE RESULTAT AVEC LA CLE PUBLIQUE DE BOB PUIS ELLE ENVOIE LE TEXTE CHIFFRÉ DEUX FOIS.
3. BOB DÉCHIFFRE LE MESSAGE GRÂCE À SA CLÉ PRIVEE PUIS DÉCHIFFRE UNE NOUVELLE FOIS AVEC LA CLÉ PUBLIQUE D'ALICE.



SEUL BOB PEUT DÉCHIFFRER LE MESSAGE
ET IL EST GARANTI QU'IL VIENT D'ALICE.

CHIFFREMENT ASYMETRIQUE ?

AVANTAGE: AUCUN ECHANGE DE SECRET PREALABLE

INCONVÉNIENT: PLUS LONG À CHIFFRER/DECHIFFRE QUE
DU CHIFFREMENT SYMETRIQUE



TLS/SSL: HANDSHAKE

- L'ECHANGE DE CLÉS SECRÈTES EST EFFECTUÉ VIA UN CHIFFREMENT ASYMETRIQUE
1. LE SERVEUR ENVOIE SA CLE PUBLIQUE (ELLE-MÊME VALIDÉE PAR LE CERTIFICAT).
 2. LE CLIENT GENÈRE UNE CLÉ SECRÈTE ET LA CHIFFRE AVEC LA CLE PUBLIQUE DU SERVEUR.
 3. LE SERVEUR DECHIFFRE LA CLE SECRÈTE AVEC SA CLE PRIVEE.



TLS RECORD

L'ECHANGE DE DONNEES CHIFFREES SYMETRIQUEMENT PEUT ENFIN COMMENCER.

AVEC QUI SUIS-JE EN TRAIN DE DIALOGUER ?

- HTTPS://EXAMPLE.COM EST RESOLU PAR MON DNS EN 93.184.216.34
- ET SI LE DNS RESOLVEUR DE MON FAI ME MENTAIT ?
- ET SI MON TRAFFIC ETAIT ROUTÉ ?

JE NE PEUX PAS FAIRE CONFIANCE UNIQUEMENT AU SERVEUR LORS DU TLS HANDSHAKE.



TLS/SSL: HANDSHAKE

LE SERVEUR ENVOIE SA CLE PUBLIQUE VALIDÉE PAR LE CERTIFICAT.

QUI VALIDE LE CERTIFICAT ?



HTTPS: LES CERTIFICATS SSL/TLS

UN TIERS DE CONFIANCE: LES AUTORITÉS DE CERTIFICATION.

IDENTRUST, COMODO, DIGICERT, GODADDY,
GLOBALSIGN, LET'S ENCRYPT, ETC.

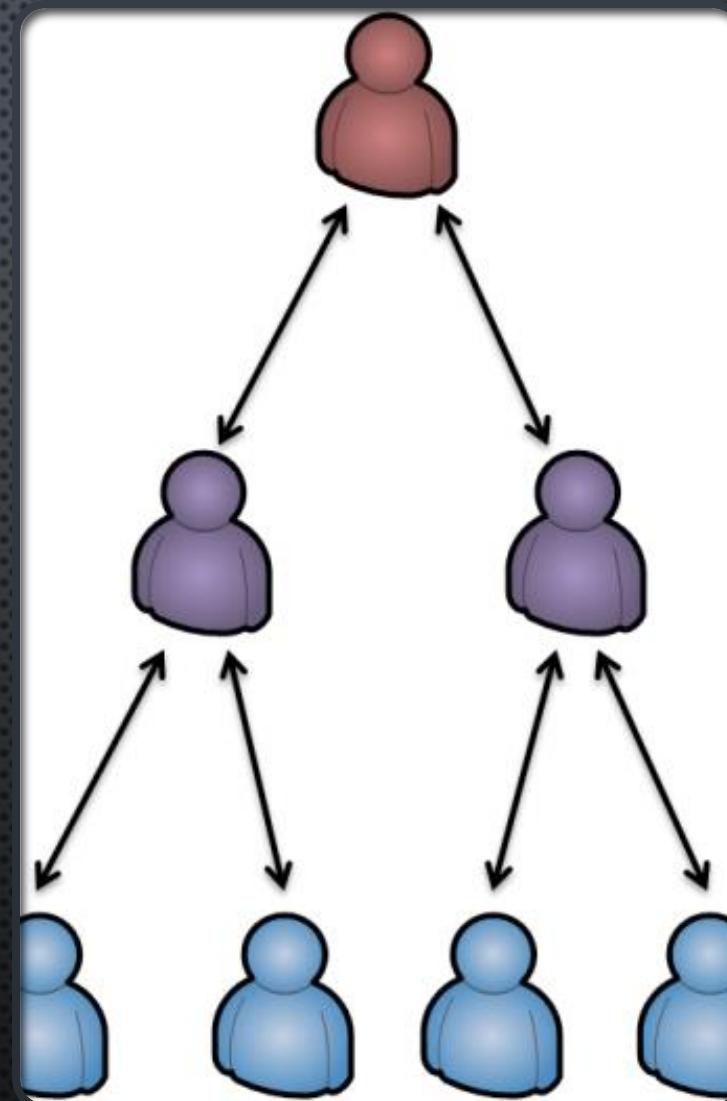
PLUS DE 65. LES 7 PREMIERES REPRÉSENTENT 99% DES CERTIFICATS EN COURS DE VALIDITÉ.

- DOMAIN VALIDATION: DROIT EXCLUSIF DU DOMAINE \$\$
- ORGANISATION VALIDATION: VÉRifie L'IDENTITÉ \$\$\$\$\$
- EXTENDED VALIDATION: VÉRifie L'ENTREPRISE\$\$\$\$\$\$\$



CERTIFICATS: LA CHAINE DE CONFIANCE

1. L'AUTORITÉ DE CERTIFICATION GÉNÈRE UN CERTIFICAT (20 ANS) SIGNÉ AVEC SA CLÉ PRIVEE.
2. LE CERTIFICAT EST INSTALLÉ DANS VOTRE SYSTÈME D'EXPLOITATION (MICROSOFT) ET VOTRE NAVIGATEUR (MOZILLA, GOOGLE).
3. LORSQUE L'AUTORITE DE CERTIFICAT VEUT SIGNER VOTRE CERTIFICAT, ELLE UTILISE UN CERTIFICAT INTERMEDIAIRE (10 ANS) DÉJÀ VALIDÉ PAR SON CERTIFICAT RACINE.
4. VOTRE NAVIGATEUR REMONTE LA CHAÎNE DE CONFIANCE DE VOTRE CERTIFICAT (1 AN) POUR SAVOIR SI IL DOIT L'ACCEPTER.



LES AUTORITES: DIGNES DE CONFIANCE ?

- DES ENTREPRISES LUCRATIVES PRIVEES MAIS AUDITEES.
- VOUS/VOTRE ENTREPRISE POUVEZ AJOUTER DES CERTIFICATS RACINE.
- UNE AUTORITE DE CERTIFICATION PEUT GENERER DES CERTIFICATS INDUS (SYMANTEC).

UN CERTIFICAT RACINE PEUT ETRE BANNI (GOOGLE, MOZILLA, MICROSOFT).



DOIS-JE UTILISER HTTPS POUR MON BLOG ?

OUI.

CONFIDENTIALITE**

INTEGRITE

RAPIDITE (HTTP 2)

SEO ++

BRUIT

GRATUIT



LET'S ENCRYPT: PRESENTATION

- AUTORITÉ DE CERTIFICATION
- ELECTRONIC FRONTIER FOUNDATION, CISCO, AKAMAI, IDENTRUST, MOZILLA ET UNIVERSITÉ DU MICHIGAN
- 2015
- FOURNI DES CERTIFICATS DOMAIN VALIDATION GRATUITS
- VALIDITÉ 90 JOURS
- AUTOMATISÉ
- TRANSPARENT (CT)
- LEVER LA BARRIERE PECUNIAIRE



LET'S ENCRYPT: MISE EN OEUVRE

PROTOCOLE ACME

- DELIVRER DES CERTIFICATS
- REVOQUER DES CERTIFICATS

PROUVER QUE L'ON POSSÈDE LE DOMAINE

- EN CHIFFRANT UN SECRET À UNE URL PARTICULIÈRE
- EN CHIFFRANT UN SECRET DANS UN ENREGISTREMENT DNS



APACHE2



```
SSLEngine on
SSLCertificateFile      /path/to/signed_certificate_followed_by_intermediate_certs
SSLCertificateKeyFile   /path/to/private/key
Header                  always set Strict-Transport-Security "max-age=15768000"

# Firefox 27, Chrome 30, IE 11 on W7, Edge, Opera 17, Safari 9, Android 5.0, and Java 8
SSLProtocol           all -SSLv3 -TLSv1 -TLSv1.1

SSLCipherSuite         ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
LY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256

# Mitigation
SSLHonorCipherOrder   on
SSLCompression        off
SSLSessionTickets     off
```

```
ssl_certificate /path/to/signed_cert_plus_intermediates;
ssl_certificate_key /path/to/private_key;
ssl_session_timeout 1d;
ssl_session_cache shared:SSL:50m;
add_header Strict-Transport-Security max-age=15768000;
```

Firefox 27, Chrome 30, IE 11 on W7, Edge, Opera 17, Safari 9, Android 5.0, and Java 8
ssl_protocols TLSv1.2;

```
ssl_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-
SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256';
```

```
# Mitigation
ssl_prefer_server_ciphers on;
ssl_session_tickets off;
```

CADDIE : LE PETIT NOUVEAU

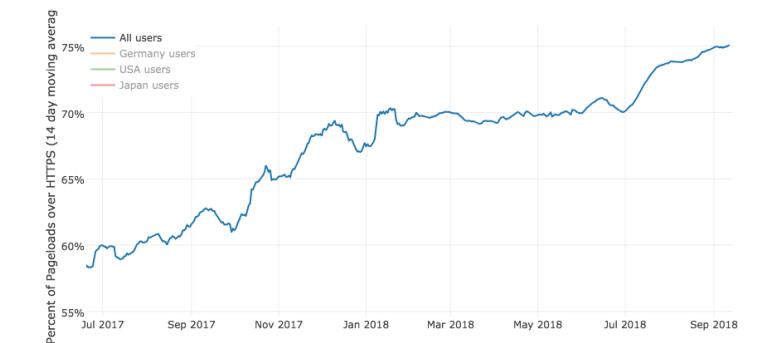
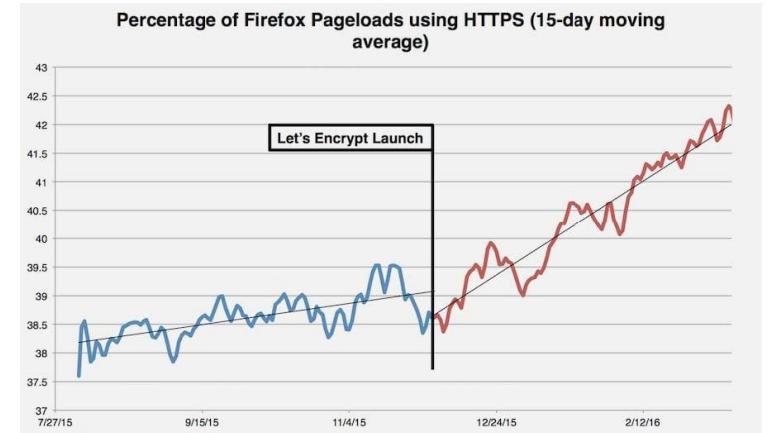
- HTTP/2
- HTTPS PAR DÉFAUT
- ACME COMPATIBLE
- KISS

```
YOURDOMAIN.COM {  
    ROOT /VAR/www  
}
```



LET'S ENCRYPT: LES RESULTATS

- 25M DE SITES WEB LA PREMIÈRE ANNÉE
- 65 MILLION SITES WEB CUMULÉS EN 2 ANS
- 500K CERTIFICATS PAR JOUR
- FIN 2018: 380M DE CERTIFICATS, 129M DE SITES WEB
- 75% DU WEB EST EN HTTPS vs. 38% EN 2015 (FIREFOX)

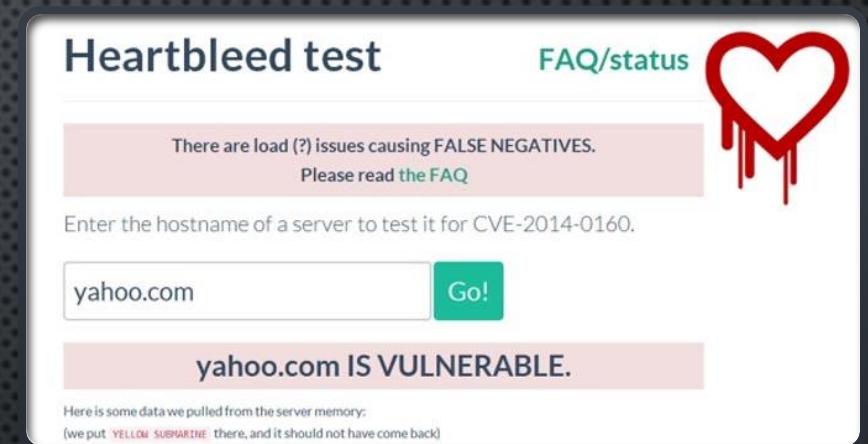


CASSER HTTPS: LES FAILLES DE SECURITE

- TLS: HEARTBLEED (2014)
- SSLv3: POODLE (2014)
- SSLv2: DROWN (2016)

CAUSES: OBSOLESCENCE / PETITE EQUIPE / RETROCOMPATIBILITE

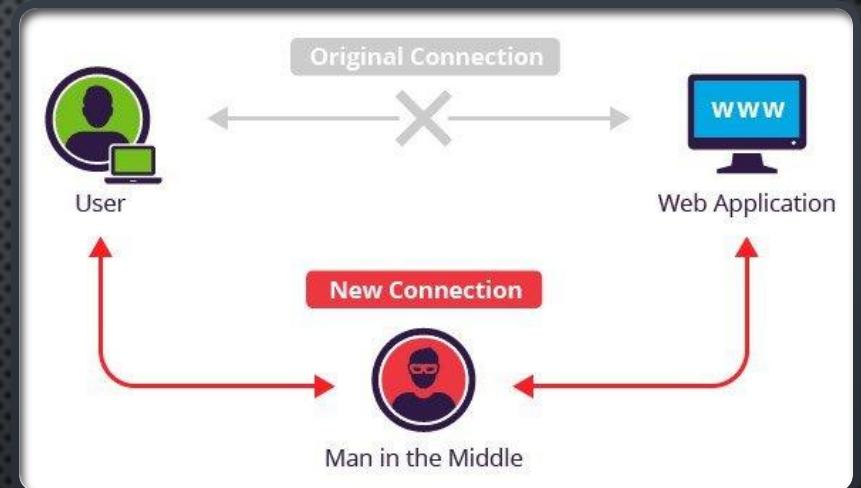
SOLUTIONS: + D'AUDIT + DE CONTRIBUTIONS + DE DIVERSITE



CASSER HTTPS: MAN-IN -THE- MIDDLE

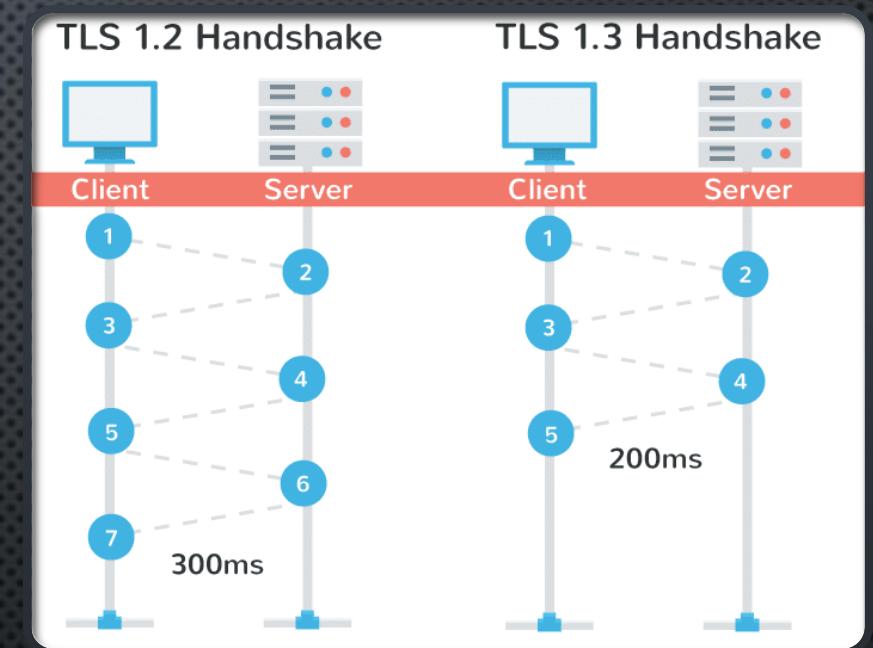
- 1. INSTALLER UN CERTIFICAT RACINE SUR LE PC CIBLE
- 2. METTRE EN PLACE UN PROXY TRANSPARENT
- 3. PROFITER !

"ANTIVIRUS INTERNET"



TLS 1.3

- ABANDON DES ALGORITHMES DE CHIFFREMENT ET DE HACHAGE OBSOLÈTES
- EMPÊCHER LE DOWNGRADE
- ACCÉLÉRER LE HANDSHAKE
- FONCTIONNALITÉS OBLIGATOIRES (PFS)



SUPPRIME LA RETRO-COMPATIBILITE

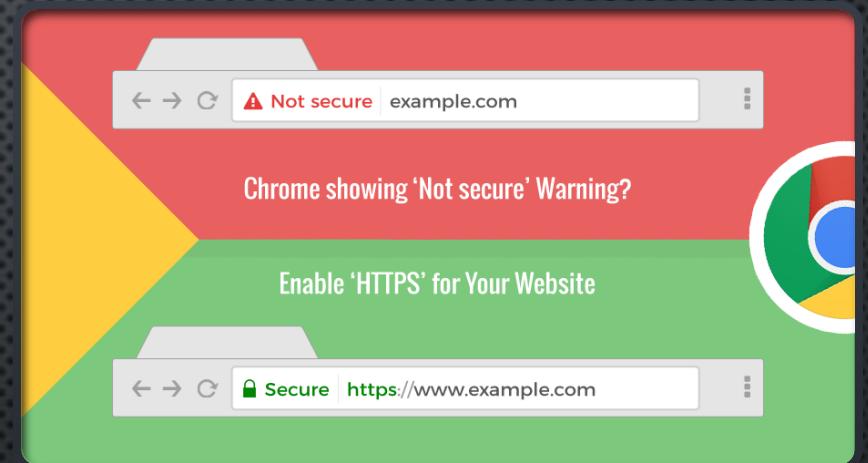
eTLS: CANADA DRY DU TLS

- INQUIÉTUDES SECTEURS BANCAIRE ET DE LA "SECURITE" D'ENTREPRISE.
- EMPÊCHE LE DÉCHIFFREMENT À LA VOLÉE ET LA SURVEILLANCE AISÉE DES CONNEXIONS (PFS)
- DEMANDE DE PORTE DÉROBÉE POUR DOWNGRADE : REFUS DE L'IETF
- CREATION DE LEUR PROPRE VERSION ENTREPRISE-TLS !



LES NAVIGATEURS: PIONNIERS DE LA SECURITE

- CHROME, SAFARI, FIREFOX: 85% DU MARCHÉ
- MONOPOLE: STANDARD DE FACTO
- RÉVOCATION DE CERTIFICATIONS
- AFFICHER DES MESSAGES INQUIÉTANTS AU CONSOMMATEUR
- METTRE LA PRESSION SUR LES COMMERCANTS



DNS: SECURISATION EN COURS

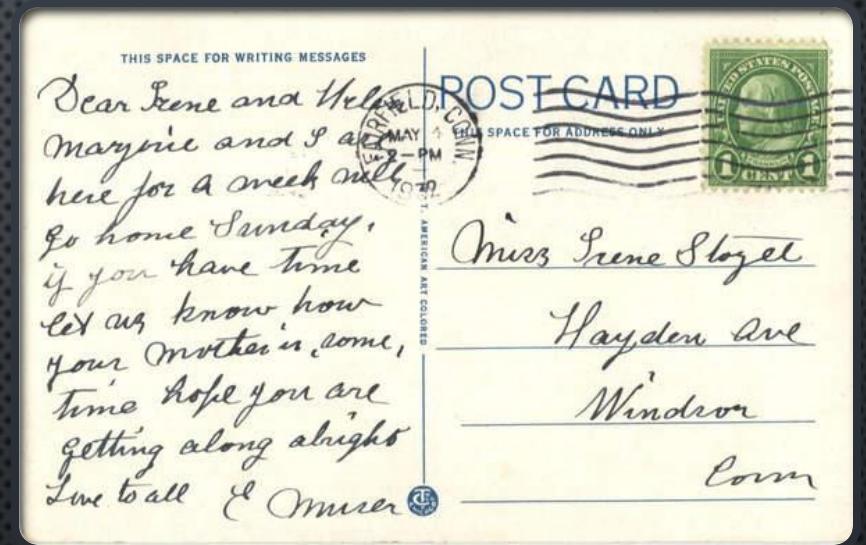
- ARCHITECTURE À CLÉ PUBLIQUES DNSSEC (2007)
- PROTOCOLE E-DNS DÉSORMAIS OBLIGATOIRE (DnsFLAGDAY 2019)

LA SÉCURISATION DU DNS EST D'IMPORTANCE CRITIQUE À LA SÉCURITÉ DE L'INTERNET DANS SON ENSEMBLE.



SECURISER SMTP ?

- PLUS VIEUX QUE HTTP (1982)
- IMPOSSIBLE D'AUTHENTIFIER L'EXPEDITEUR
- IMPOSSIBLE DE GARANTIR LE CHIFFREMENT DU TRANSPORT
- TRÈS COMPLIQUÉ À METTRE À JOUR GLOBALEMENT
- MATÉRIEL/LOGICIEL OBSOLETE
- CHIFFREMENT À LA DEMANDE : STARTTLS
- CHIFFRER DES MESSAGES
- SIGNER LES MESSAGES (DKIM)
- SMTPS ONLY



ET LE E-COMMERCE ?

- NORME DE SÉCURITÉ POUR LES PRESTATAIRES DE PAIEMENT
- VISA, MASTERCARD, AMERICAN EXPRESS, DISCOVER CARD, JCB
- 2004
- EXIGENCES DE CONFORMITÉ
- AUDITS TRÈS FRÉQUENTS
- PCI-DSS REQUIERT TLS1.2 DEPUIS JUILLET 2018



CONCLUSION

- HTTPS GARANTI LA SECURITÉ DE LA CONNEXION ENTRE LE CLIENT ET LE SERVEUR.
- HTTPS NE GARANTI PAS TOTALEMENT L'IDENTITE DU SERVEUR.
- HTTPS EST AUSSI UTILE POUR VOTRE BLOG.
- LES AUTORITÉS DE CERTIFICATION NE SONT PAS LA PANACÉE
- VOTRE NAVIGATEUR/SERVEUR CHOISIRA TOUJOURS LE PROTOCOLE LE PLUS SECURISE SI DISPONIBLE (TLS1.3)
- LA SECURITÉ DE HTTPS ET SMTPS EST LIÉE À DNSSEC.



MERCI DE VOTRE
ATTENTION

15MN QUESTIONS/REPONSES