

Exercise : SSL/TLS

HTTPS (HTTP sur SSL/TLS) permet sécuriser les communications entre un serveur Web et un navigateur. La figure ci-dessous présente des paquets capturés chez un client web (navigateur) qui accède au site www.google.tn (la première colonne donne les numéros des paquets capturés).

Le navigateur calcule une clé secrète K (master key) et l'envoi au serveur dans un canal sécurisé.

No.	Time	Source	Destination	Protocol	Length	Info
15	0.545613000	192.168.1.4	193.95.57.20	DNS	73	Standard query 0xae9a A www.google.in
16	0.566743000	193.95.57.20	192.168.1.4	DNS	475	Standard query response 0xae9a A 193.95.13.57 A 193.95.13.59 A 193.95.13.16 A 193.95.13.20 A 193.95.13.28 A 193.95.13.32 A 193.95.13.34 A 193.95.13.36 A 193.95.13.38 A 193.95.13.40 A 193.95.13.42 A 193.95.13.44 A 193.95.13.46 A 193.95.13.48 A 193.95.13.50 A 193.95.13.52 A 193.95.13.54 A 193.95.13.56 A 193.95.13.58 A 193.95.13.60 A 193.95.13.62 A 193.95.13.64 A 193.95.13.66 A 193.95.13.68 A 193.95.13.70 A 193.95.13.72 A 193.95.13.74 A 193.95.13.76 A 193.95.13.78 A 193.95.13.80 A 193.95.13.82 A 193.95.13.84 A 193.95.13.86 A 193.95.13.88 A 193.95.13.90 A 193.95.13.92 A 193.95.13.94 A 193.95.13.96 A 193.95.13.98 A 193.95.14.00 A 193.95.14.02 A 193.95.14.04 A 193.95.14.06 A 193.95.14.08 A 193.95.14.10 A 193.95.14.12 A 193.95.14.14 A 193.95.14.16 A 193.95.14.18 A 193.95.14.20 A 193.95.14.22 A 193.95.14.24 A 193.95.14.26 A 193.95.14.28 A 193.95.14.30 A 193.95.14.32 A 193.95.14.34 A 193.95.14.36 A 193.95.14.38 A 193.95.14.40 A 193.95.14.42 A 193.95.14.44 A 193.95.14.46 A 193.95.14.48 A 193.95.14.50 A 193.95.14.52 A 193.95.14.54 A 193.95.14.56 A 193.95.14.58 A 193.95.14.60 A 193.95.14.62 A 193.95.14.64 A 193.95.14.66 A 193.95.14.68 A 193.95.14.70 A 193.95.14.72 A 193.95.14.74 A 193.95.14.76 A 193.95.14.78 A 193.95.14.80 A 193.95.14.82 A 193.95.14.84 A 193.95.14.86 A 193.95.14.88 A 193.95.14.90 A 193.95.14.92 A 193.95.14.94 A 193.95.14.96 A 193.95.14.98 A 193.95.15.00 A 193.95.15.02 A 193.95.15.04 A 193.95.15.06 A 193.95.15.08 A 193.95.15.10 A 193.95.15.12 A 193.95.15.14 A 193.95.15.16 A 193.95.15.18 A 193.95.15.20 A 193.95.15.22 A 193.95.15.24 A 193.95.15.26 A 193.95.15.28 A 193.95.15.30 A 193.95.15.32 A 193.95.15.34 A 193.95.15.36 A 193.95.15.38 A 193.95.15.40 A 193.95.15.42 A 193.95.15.44 A 193.95.15.46 A 193.95.15.48 A 193.95.15.50 A 193.95.15.52 A 193.95.15.54 A 193.95.15.56 A 193.95.15.58 A 193.95.15.60 A 193.95.15.62 A 193.95.15.64 A 193.95.15.66 A 193.95.15.68 A 193.95.15.70 A 193.95.15.72 A 193.95.15.74 A 193.95.15.76 A 193.95.15.78 A 193.95.15.80 A 193.95.15.82 A 193.95.15.84 A 193.95.15.86 A 193.95.15.88 A 193.95.15.90 A 193.95.15.92 A 193.95.15.94 A 193.95.15.96 A 193.95.15.98 A 193.95.16.00 A 193.95.16.02 A 193.95.16.04 A 193.95.16.06 A 193.95.16.08 A 193.95.16.10 A 193.95.16.12 A 193.95.16.14 A 193.95.16.16 A 193.95.16.18 A 193.95.16.20 A 193.95.16.22 A 193.95.16.24 A 193.95.16.26 A 193.95.16.28 A 193.95.16.30 A 193.95.16.32 A 193.95.16.34 A 193.95.16.36 A 193.95.16.38 A 193.95.16.40 A 193.95.16.42 A 193.95.16.44 A 193.95.16.46 A 193.95.16.48 A 193.95.16.50 A 193.95.16.52 A 193.95.16.54 A 193.95.16.56 A 193.95.16.58 A 193.95.16.60 A 193.95.16.62 A 193.95.16.64 A 193.95.16.66 A 193.95.16.68 A 193.95.16.70 A 193.95.16.72 A 193.95.16.74 A 193.95.16.76 A 193.95.16.78 A 193.95.16.80 A 193.95.16.82 A 193.95.16.84 A 193.95.16.86 A 193.95.16.88 A 193.95.16.90 A 193.95.16.92 A 193.95.16.94 A 193.95.16.96 A 193.95.16.98 A 193.95.17.00 A 193.95.17.02 A 193.95.17.04 A 193.95.17.06 A 193.95.17.08 A 193.95.17.10 A 193.95.17.12 A 193.95.17.14 A 193.95.17.16 A 193.95.17.18 A 193.95.17.20 A 193.95.17.22 A 193.95.17.24 A 193.95.17.26 A 193.95.17.28 A 193.95.17.30 A 193.95.17.32 A 193.95.17.34 A 193.95.17.36 A 193.95.17.38 A 193.95.17.40 A 193.95.17.42 A 193.95.17.44 A 193.95.17.46 A 193.95.17.48 A 193.95.17.50 A 193.95.17.52 A 193.95.17.54 A 193.95.17.56 A 193.95.17.58 A 193.95.17.60 A 193.95.17.62 A 193.95.17.64 A 193.95.17.66 A 193.95.17.68 A 193.95.17.70 A 193.95.17.72 A 193.95.17.74 A 193.95.17.76 A 193.95.17.78 A 193.95.17.80 A 193.95.17.82 A 193.95.17.84 A 193.95.17.86 A 193.95.17.88 A 193.95.17.90 A 193.95.17.92 A 193.95.17.94 A 193.95.17.96 A 193.95.17.98 A 193.95.18.00 A 193.95.18.02 A 193.95.18.04 A 193.95.18.06 A 193.95.18.08 A 193.95.18.10 A 193.95.18.12 A 193.95.18.14 A 193.95.18.16 A 193.95.18.18 A 193.95.18.20 A 193.95.18.22 A 193.95.18.24 A 193.95.18.26 A 193.95.18.28 A 193.95.18.30 A 193.95.18.32 A 193.95.18.34 A 193.95.18.36 A 193.95.18.38 A 193.95.18.40 A 193.95.18.42 A 193.95.18.44 A 193.95.18.46 A 193.95.18.48 A 193.95.18.50 A 193.95.18.52 A 193.95.18.54 A 193.95.18.56 A 193.95.18.58 A 193.95.18.60 A 193.95.18.62 A 193.95.18.64 A 193.95.18.66 A 193.95.18.68 A

1. Que représentent les paquets 15, 16, 17 et 18 ?
2. Que représentent les paquets 19, 20 et 21 ?
3. Que représentent les paquets 26, 27 et 28 ?
4. Sur son navigateur, l'utilisateur a tapé l'adresse <http://www.google.tn> ou <https://www.google.tn> ? Expliquer.
5. Préciser, à l'aide d'un schéma, les différents messages échangés pour établir une connexion sécurisée entre le client et www.google.tn
6. Pourquoi on n'utilise pas directement le chiffrement asymétrique pour sécuriser les communications HTTPS ? Donner deux raisons.
7. La clé K (Premaster key) est-elle envoyée au serveur dans un canal sécurisé et authentifié ? expliquer ?
8. Pourquoi certains anciens navigateurs web ne peuvent pas utiliser HTTPS ?

9. À votre avis, la clé privée du serveur web est stockée en clair ou protégé par mot de passe ? Expliquer.

10. Il est possible d'utiliser un certificat client stocké sur le navigateur pour l'échange HTTPS. Donnez un avantage et un inconvénient de procéder ainsi.