Sources commentées

Liens/sources	Ce qu'on a retenu de ce cours
Questions posés à un professionnel du monde des Réseaux et Télécommunications	Les principes de codage asymétrique, le principe de clé publique/privées, principe de tier de confiance (Autorité de certification), http, https, exemple concret, les formules mathématiques RSA (qu'on ne va pas utiliser)
https://www.youtube.com/watch?v=_6ukY5p6vTY	→ explication du chiffrement symétrique (dans le cas du code de césar) avec le soucis de la cryptanalyse (étude des messages chiffré pour retrouver le message d'origine sans posséder la clé de chiffrement). C'est pour ça qu'on fait des chiffrements symétriques complexes (AES). Explication de l'interception de la clé par un éventuel hacker On préfère donc utiliser le déchiffrement asymétrique, méthode RSA. On a alors une clé pour chiffrer (clé publique) et une autre pour déchiffrer (clé privée). • Clé publique peut crypter et pas décrypter • Clé privée peut décrypter mais pas crypter RSA plus lent que AES avec des messages plus longs alors temps de transmission plus long.
https://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/	Schéma descriptif de RSA. Principe de base de la cryptologie asymétrique mais surtout symétrique. Formules mathématiques à démonter ???
https://www.youtube.com/watch?v=MuNyEoU5tSo	Cryptographie asymétrique dans le transfert de données, les formules

	mathématiques avancés (qu'on n'utilise pas non plus). La constitution d'une clé avec les nombres premiers.
https://aboutssl.org/how-https-and-ssl-works/	Requête entre le serveur web et le navigateur lors d'une communication. Le serveur web communique sa clé publique mais garde sa clé privée secrète et uniquement pour lui Le navigateur créé une troisième clé appelée clé session La clé session est encryptée par le navigateur Chiffrement asymétrique remplacé par chiffrement symétrique Clé session valide jusqu'à déconnexion du site. SSL est un protocole standard utilisé dans HTTPS. La nouvelle version s'appelle TLS : Transport Layer Security. Pour crypter des données : - Choix algorithme de cryptage entre le navigateur et le serveur. - La récupération clé de cryptage.
https://fr.wikipedia.org/wiki/Tiers_de_confiance	Définition simple d'un tier de confiance, et les différents groupement (qu'on n'a pas gardé)
Sec'num "module 4 - L'envers du décor d'une connexion web"	Requête http, HTTPS et le cadenas, Exemple avec le payement en ligne avec le protocole SSL TLS, importance de HTTPS avec son principe de fonctionnement entre un navigateur et serveur. Le certificat d'un serveur HTTPS

- Ce qu'on a retenu vis-à-vis de ce sujet :
  - 3 parties :
    - La différence entre http et https.
    - A quoi correspondent les clés publiques et privés.
    - Utilité des tiers de confiance lors d'une communication sécurisée
  - Le fonctionnement d'http et https :
    - http moins sécurisé avec des données pas cryptées.
    - https : extension d'http avec l'ajout d'une couche TLS/SSL qui permet d'ajouter une sécurité en plus, car les données sont crypté

le long de la communication donc le hacker a plus de mal pour les voler.

- Le cryptage symétrique et ses problèmes
    - Décrypter et crypter avec la même clé donc le hacker tout intercepter et modifier et servir de passerelle.
- Le cryptage asymétrique et ses problèmes :
    - Sans tier de confiance il y a le même problème que symétrique car ce hacker peut donner sa clé publique.
- Le contenu de chaque partie avec des éléments intéressant tel que des exemples : entre A et B qui veulent communiquer et le hacker qui veut intercepter ces données.
- La notion de tier de confiance, avec les différentes autorités, et le rôle de l'ANSSI en France.
- La comparaison simple entre certificat et passeport ainsi que tier de confiance et administration qui donne le passeport.
- Ce que contient le contrat d'un tier de confiance (la clé public, l'identité de celui qui possède la clé publique, la date de validité et signature).
- Une ouverture du sujet avec la notion d'ordinateur quantique.
- La façon de simplifier des termes qui paraissent dur mais qui au final ne le sont pas tant que ça.