13. Expliquer l'évolution historique de la notion de clé de chiffrement. En particulier, expliquer les termes de "substitution", "transposition", "chiffrements polyalphabétiques", "grille de Vigenère", "chiffrement de blocs", "padding", "clé publique", "clé secrète", "clé privée", "protocole de Diffie-Fellman", "AES", "RSA". Que penser de l'affirmation : "les systèmes de chiffrement actuels sont forcément vulnérables, puisque les algorithmes qu'ils utilisent sont publics" ? Quels sont, parmi ces termes, ceux que l'on retrouve dans la programmation des questions de chiffrement et d'authentification ?

a cryptographie voit le jour vers 1900 av. J.C. en égypte par l'utilisation de hiéroglyphes non standards notamment. Ceci dit, on cite généralement pour débuter l'histoire de la cryptographie le code de Cesar (-50 av. J.C.). Il est basé sur le principe de substitution de caractères : remplacer chaque lettre du message par celle qui se trouve x positions plus loin dans l'alphabet. On dit encore que la clé de cryptage est le nombre de position. Une telle clé doit évidemment rester secrète. La clé est utilisée dans un algorithme de cryptage (décaler les lettres de X position). Cet algorithme de cryptage est public, c'est la connaissance de la clé qui est fondamentale, pas celle de l'algorithme.

Code de César : a b c d e …
l l l l l …
z a b c d …

Ici la clé est 1, en effet, chaque lettre a été substitué par la lettre +1 dans l'alphabet. Cette technique de chiffrement est assez facile à décodé néanmoins. Effectivement, elle ne résiste pas à une analyse fréquentielle.

Un autre algorithme de chiffrement qui a vu le jour durant cette même période, est l'algorithme de transpositon, qui consiste à transposé certaine partie du message à une autre place. Comme exemple, transposer 2 lettres successives et laissé la 3eme intacte, ce qui nous donne :
Mot d'origine = nicolas —-> incloas = mot transposé
La clé sera donc 2/3 par exemple, pour indiquer que les lettres ont été transposé 2 par 2 et que la 3eme reste intacte. Malgré cela, il reste assez simple de cassé le codage, en effet, la phrase est facile a retrouver.

Pour compliqué le codage, la transposition et la substitution peuvent être appliqué ensemble.
La clé numérique à été remplacer par une phrase, ce qui endurci le codage. Alors est apparu les algorithme de génération de clé. Assez simple dans un premier temps, il s'agissait par exemple d utiliser les premiers mots de verset de la bible en fonction du jour de l'année.

Nous nous retrouvons donc ici, avec un chiffrement symétrique, en effet la même clé est utilisé pour chiffrer et pour déchiffrer.

Ceci dit, ces méthodes de cryptographies restaient assez simples et vite cassée. La renaissance offre à son tour ses nouvelles idées dans ce domaine avec le chiffrement polyalphabétique.
L'idée est de changer d'alphabet crypté en cours de cryptage d'un message. Mr Alberti réalisa cela à l'aide de cadran chiffreur qui met en correspondance l'alphabet clair (sur le disque extérieur) et l'alphabet crypté (sur le disque intérieur). Pour l'utiliser, il suffisait de connaître une correspondance lettre claire/lettre cryptée. Bien entendu, cette correspondance changeait en cours de chiffrement.

Ensuite vint la grille de Blaise de Vigenère. Cela consistait à recopier la clé le nombre de fois nécessaire en dessous du texte clair. La lettre de la clé fixe donnait la ligne et la lettre du message donnait la colonne : la lettre retrouvé dans la grille (matrice) donnait la lettre cryptée.

On utilisa ensuite la transposition avec la substitution, combinée à un mécanisme de découpe en bloc.

Le problème venait du fait que tous les blocs n'étaient pas toujours remplis. On aurait pu les compléter par un autre caractère mais cela aurait donné une information au cryptoanalyste.
Pour éviter cela, ils utilisèrent un algorithme de remplissage (padding) qui permit de générer des caractères de remplissage qui ne furent pas détectable trop facilement.

ECB (Electronic Code Book) : un bloc de teste clair ce chiffre en un bloc de texte chiffré, indépendamment des autres blocs.
CBC (Cipher Bloc Chaining) : chaque bloc de texte clair est combiné par un XOR avec le bloc de texte chiffré précédent.

Jusqu'ici, on a supposé que les deux parties de la communication cryptée était en possession de la clé secrète (phrase, mot, nombre…) qui assurait la confidentialité. Celle-ci était donc la clé de chiffrement. Ceci dit, cette hypothèse n'est pas forcément facile à satisfaire. En 1970, Diffie et Hellman élaborèrent un protocole d'échange ; basé sur l'arithmétique modulaire, permettant de s'accorder sur une clé secrète sur base d'une discutions publique. Ce protocole fait ainsi intervenir les concepts de clé privée et clé publique. En effet, grâce à un nombre inconnu de chaqu'un des coté, une clé secrète peut être trouvé sans échanger directement cette clé.

Le concept de clé privée/publique trouve son implémentation concrète dès 1978 avec le système RSA. Ce système de communication sécurisée, basé sur la difficulté de factoriser les grands nombres consiste à

a) Crypter un message par un expéditeur avec la clé publique (donc connue de tous) du destinataire.
b) Décrypter le message par son destinataire qui utilise la clé privée associée à la clé publique qui a servi à crypter et qu'il est le seul à posséder.

Autrement dit, la clé qui sert à crypter n'est pas celle qui sert à décrypter. Ce concept est toujours utilisé actuellement.

AES et Rijndael (nom donnée a partir des noms des concepteurs Belge) remplace l'algorithme DES. Rijndael utilise des des clés multiples de 32 bits dans l'intervalle [128,256] alors que AES en est un sous-ensemble se limitant à des clés de 128, 192 ou 256 bits.

"les systèmes de chiffrement actuels sont forcément vulnérables, puisque les algorithmes qu'ils utilisent sont publics »

Les systèmes de chiffrement actuels sont pour le moment incassable, ou du moins, pas dans des temps raisonnable. En effet ceux-ci se basse sur des algorithmes modulaire, qui donne des résultats erratique et donc non réversible. Même si ceux-ci sont publique, cela ne pose pas de problème si le pirate connait la formule de la réponse car celui-ci n'arrive pas à faire marche arrière avec cette algorithme. La force des chiffrement actuelle n'est pas dans le secret des algorithme utilisé mais dans la complexité de la clé. Les algorithme de génération de clé est donc indisponible pour générer une clé non duplicable !

Nous retrouvons dans la programmation ces termes :
« chiffrement de blocs », « padding », « clé publique » , « clé secrète » , « clé privée » , « diffie-Hellman » , « AES » , « RSA ».