Semestre 2 Master 1 Informatique : Option R&S Cours Introduction à la sécurité

Examen : Introduction à la Sécurité

Documents non autorisés/ durée 2h00mn

Questions :

1) Faire la matrice de risque à 4 niveaux (4 lignes et 4 colonnes) puis donner :
   a. Le risque le plus critique
   b. Le risque le moins critique
   c. Sur quel(s) paramètre(s) agir si on doit mener un plan de prévention sur le risque le plus critique ?
2) Donner deux mécanismes de sécurité permettant de mettre en œuvre l'authentification
3) On considère un système de chiffrement par Vigenère utilisant la clé K=UGB. Trouvez la clé de déchiffrement K^{-1}.
4) Avec le chiffrement par transposition utilisant la clé K=[3-4-1-2], un texte chiffré C (ou cryptogramme) donne MASTER.
   a. Quel est le texte clair correspondant ?
   b. Donner la clé inverse K^{-1} permettant de déchiffrer.
5) On considère les systèmes de chiffrement suivants sur des lettres alphabétiques où la robustesse est mesurée en fonction du nombre maximum de clés possibles :
   - Un système de chiffrement utilisant la méthode de César.
   - Un système de chiffrement utilisant la substitution mono-alphabétique.
   - Un système de chiffrement utilisant une clé de transposition de 3 lettres.
   - Un système de chiffrement utilisant une clé de Vigenère de 3 lettres.

   Classer les par ordre de robustesse
6) Soient les 4 blocs de 5 bits suivants à chiffrer dans cet ordre : 10111 10111 10111 10111
   a. Quelle(s) sont les attaque(s) possible(s) si le chiffrement ECB est utilisé ?
   b. Quelle(s) sont les attaque(s) possible(s) si le chiffrement CBC est utilisé ?
7) A et B souhaitent publiquement se partager une clé commune Kab sans à priori avoir connaissances d'informations communes. Décrire deux techniques (ou protocoles) qui peuvent être utilisées pour partager Kab
8) Analyser ligne par ligne et trouver les propriétés (services ou objectifs de sécurité) que comporte ce protocole suivant sachant que : pkA et pkB sont respectivement les clés publiques de A et B ; prkA et prkB les clés privées de A et B ; mA et mB des messages

   $A \rightarrow B$: A,{Na}pkB.
   $B \rightarrow A$: B,{Na.Nb}pkA.
   $A \rightarrow B$: A,{Nb,Kab}pkB
   $A \rightarrow B$: A,{**mA**}Kab
   $B \rightarrow B$: B,{**mB**}Kab
9) Analyser et trouver les propriétés (services ou objectifs de sécurité) que comporte ce protocole suivant sachant que : pkA et pkB sont respectivement les clés publiques de A et B ; prkA et prkB les clés privées de A et B ; m un message.

   $A \rightarrow B$: A, {{**mA**}prKA}pkB.
   $A \rightarrow B$: B, {{**m**}prKB}pkA.
10) Analyser et trouver les propriétés (services ou objectifs de sécurité) que comporte ce protocole suivant sachant que : H est une fonction de hachage : m un message.

   $A \rightarrow B$: A, m, H(m)
11) A et B se partagent à priori une valeur secrète X, analyser et trouver les propriétés (services ou objectifs de sécurité) que comporte ce protocole suivant sachant que : H est une fonction de hachage, || l'opérateur de concaténation et m un message.

   $A \rightarrow B$: A, m, H(m||X)
   $A \rightarrow B$: B, {{**m**}prKB}pkA.

Bonne chance