Sécurité des SI

TD3 (cryptographie)

1) Expliquez les concepts qui sont à la base d'un schéma de Feistel.
2) Les fonctions de hachage permettent de construire des clés hierarchiques. Essayez de généraliser le schéma lorsque les niveaux de sécurité admettent un ordre partiel (certains niveaux ne peuvent pas être comparés).
3) Alice part en conférence à l'étranger et veut se connecter à l'INRIA pendant son séjour. L'INRIA exige qu'Alice utilise un nouveau password à chaque nouvelle connexion. Avant de partir, Alice choisit un nombre aléatoire w et hache cette valeur t+1 fois afin d'obtenir une valeur qu'elle donne au système. Elle garde tous les hachés sur une clé USB qu'elle emporte à la conférence avec elle. Sur le lieu de la conférence, Elle décide de se connecter, proposez un protocole qui lui permette de se connecter t fois avec à chaque fois un nouveau password.
4) Pour tout chiffrement par block, le fait qu'il soit non linéaire est crucial pour sa sécurité. Considérons un système de chiffrement par block nommé EL qui chiffre des blocks de 128 bits pour produire des chiffrés de 128 bits. Puisque le chiffrement est linéaire, on a EL(k,[m1+m2]) = EL(k,m1)+EL(k,m2) pour tous m1 et m2. Décrivez comment, en choisissant 128 chiffrés et en obtenant le texte clair correspondant à chacun d'eux, un adversaire peut décrypter tout chiffré sans connaître la clé k.
5) Comme vu en cours, ECBC-MAC utilise un mode CBC et divise le message en blocs de taille identique. Supposons que la taille du message ne soit pas exactement un multiple de la taille des blocs. Dans ce cas il faut faire un « padding », c'est à dire rajouter des bits dans le dernier bloc. Supposons que l'on rajoute des bits à 0. Cette solution est-elle adéquate ? Proposez un padding sûr. Analysez votre padding et essayez de l'optimiser afin que on ne soit jamais obligé d'ajouter un « dummy block ».
6) Cherchez sur Internet des information sur le Cipher-based Message Authentication Code (CMAC). Essayez de comprendre son fonctionnement et rédigez une présentation brève de CMAC.
7) On considère 16 documents (D1,...,D16). Expliquez comment on prouve, en utilisant un arbre de Merkle que D5 fait bien partie des 16 documents.