Examen UE Sécurité

Mardi 13 Novembre 2007 : 10 h – 12 h
Durée : 2 heures
Répondre en français. (Les réponses en anglais sont autorisées pour les anglophones).
Aucun document n'est autorisé. Les petites calculettes sont autorisées, mais ne sont pas indispensables.
Les réponses à chaque question doivent être courtes (se limiter au strict nécessaire).

1. Question Généralités (2 points)

1a - Quels objectifs de sécurité veut-on atteindre lorsque l'on sécurise un fichier en le chiffrant ? Quelles fonctions de sécurité utilise-t-on ? Quels mécanismes utilise-t-on ? (3 lignes maxi)
1b - Quels objectifs de sécurité veut-on atteindre lorsque l'on sécurise un fichier en le signant ? Quelles fonctions de sécurité utilise-t-on ? Quels mécanismes utilise-t-on ? (3 lignes maxi)

2. Question Biométrie (1 point)

Quelle est la fonction de sécurité assurée par la biométrie ? (1 ligne maxi)
Quels sont les avantages et les inconvénients actuels des méthodes biométriques en sécurité ? (4 lignes maxi)

3. Question Pare-feu, Système de Détection d'Intrusion et Pot de miel (3 points)

Définir simplement un pare-feu (firewall), un système de détection d'intrusion (IDS/IPS), un pot de miel (Honey pot) et une DMZ (zone démilitarisée). (10 lignes maxi)
Faire un schéma pour représenter ces dispositifs et ces notions dans une architecture de réseaux interconnectés avec Internet et un réseau d'entreprise.

4. Question méthodologie et politique de la sécurité (2 points)

Que signifie, au sens des ITSEC, un niveau d'assurance de niveau E3 ?
Quelle est la différence entre une politique de sécurité discrétionnaire (discretionary policy) et une politique de sécurité obligatoire (mandatory policy) ? Donner un exemple de chacune de ces 2 politiques.

5. Question Techniques de sécurité (2 points)

Quelle est la différence entre la stéganographie et le tatouage ? (5 lignes maxi)

6. Question protocole cryptographique (1 point)

Définir SSL/TLS (3 lignes maxi).

7. Question protocole cryptographique (2 points)

Définir et décrire IPSec (7 lignes maxi).

8. Question Infrastructure de gestion de clés et Certificats (2 points)

Quelle est la fonction principale d'une IGC (PKI – Public Key Infrastructure) ?
Définir un certificat (X509 ou SPKI) de sécurité, préciser sa fonction et son mécanisme.
(10 lignes maxi)

9. Question sur les Attaques (1 point)

Définir une attaque de rejeu (replay) et une attaque de « l'homme par le milieu » (Man in the Middle Attack) et expliquer comment on peut contrecarrer ces deux attaques.

10. Questions RSA (4 points)

On utilise les notations habituelles du RSA : p,q, n, phi, e, d
n= pq, phi = (p-1)(q-1), ed = 1 mod phi
On chiffre le message m qui devient le message c.

4a (2 points) - Astrid utilise pour clé publique : (121, 899)
Écrire les formules de chiffrement et déchiffrement.
Calculer p,q, phi et d. Chiffrer le message m = 2 avec la clé privée.

4b (1 point) - Astrid a choisi pour clé publique (121, 899). Y a-t-il d'autres solutions possibles ?
Est-ce que e = 289 et d = 529 est un couple possible de clés de chiffrement-déchiffrement ? ($289 = 17^2$; $529 = 23^{2)}$

4c (1 point) - Astrid choisit maintenant e = 13 * 17 = 221. Est-ce possible ? Si oui, calculer d.
Chiffrer le message m = 2 avec la clé publique e.
Déchiffrer le message c ainsi trouvé (donner la formule).

Remarque 1 : On donne les nombres premiers jusqu'à 1000.

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013

Remarque 2 : On donne certaines exponentiations modulaires de 2.
$2^{120} \bmod 899 = 807$
$2^{360} \bmod 899 = 745$
$2^{121} \bmod 840 = 632$
$2^{361} \bmod 840 = 632$
$715^{360} \bmod 899 = 342$
$715^{121} \bmod 899 = 591$
$2^{220} \bmod 899 = 745$
$591^{821} \bmod 899 = 2$