TTM4135 Information Security Exam June 6, 2005 --- solutions

1-25

Question	*Choice*		
	a	b	c
1		✓	
2	✓		
3			✓
4		✓	
5		✓	
6			✓
7			✓
8	✓		
9	✓		
10	✓		
11			✓
12			✓
13	✓		
14			✓
15	✓		
16	✓		
17		✓	
18		✓	
19		✓	
20			✓
21	✓		
22			✓
23	✓		
24		✓	
25	✓		

26. The recommendation X.509, part of the X.500 directory service recommendations, defines a format for public-key certificate that can be issued in a hierarchy of certification authorities. Figure 4.3 shows the formats.
27. 1) Verifiable signature 2) Within validity period.
28. Revocation because : 1) Change of authorization, for instance signer is not at the company anymore. 2) A private key is compromised or lost. 3) Certification system update, for instance algorithmic changes.
29. Invalidation by: 1) Time period expiration. or revocation list (CRL): 2) Revocation of issuer's public key. 3) Revocation of subject's public key.
30. See Section 5 of Security Lab Assignment, and Figure 4.4 in text book.
31. See textbook Figure 7.6.
32. Alice randomly selects two large prime number p and q, and computes $n := p*q$. Then she randomly selects d, conditioned on that d is relative prime to $phi(n)$ and $0<d<phi(n)$. Alice must keep p, q and d secret.
33. Alice must provide Bob with her public key (e, n), where $e := d$^-1 mod $phi(n)$. Bob verifies by checking whether (s^e mod $n = m$).
34. If there are no restrictions on m* then there are no restrictions on s*. Bob starts with a random s* and computes m* := s*^e mod n.
35. The hash function should satisfy: 1) Accept any length input. 2) Fixed length output. 3) 'Easy' to compute $y := h(x)$. 4) Onewayness: 'Hard' to compute x given $h(x)$. 5) Strong collision-free: 'Hard' to find a pair ($x1$, $x2$) such that $h(x1) = h(x2)$.
36. Make $h()$ public. In signing and verification replace m with $h(m)$.
37. Alice computes E(K,m) and sends the result (c, t) to Bob. Bob decrypts the message m by computing c/t^k mod p.

sfm 20050606.