CSC 774 Network Security

Spring 2004

Solutions to Mid-term exam #2

1. B
2. A
3. B
4. E
5 (a) m1, m2; (b) m1, o
6. (a)

P_j	P_{j+1}	P_{j+2}	P_{j+3}	P_{j+4}	P_{j+5}	P_{j+6}
i+5	i+6	i+7	i+7	U	U	U

(b) Yes. Use the TESLA immediate authentication mechanism.
7. (a) S2, P10, P8, P6, P5, P4, P2, P1
(b) S2, P10
8. # encryption: 3; # decryption: 3.
9. (a) $\{\alpha^{N1N2N3N4}, \alpha^{N1N2N3}, \alpha^{N1N2N4}, \alpha^{N1N3N4}, \alpha^{N2N3N4}\}$
(b) $\{\alpha^{N2N3N4N5N6N7}, \alpha^{N1N3N4N5N6N7}, \alpha^{N1N2N4N5N6N7}, \alpha^{N1N2N3N5N6N7}, \alpha^{N1N2N3N4N6N7}, \alpha^{N1N2N3N4N5N7}\}$; $\alpha^{N1N2N3N4N6N7}$
10. (a) K_{456}, $K_{1\text{-}9}$, $K_{1\text{-}c}$
(b)
GM → $\{u_4\}$: $\{K_{4,6}\}K_4$, $\{K_{1\text{-}4,6\text{-}9}\}K_{4,6}$, $\{K_{1\text{-}4,6\text{-}c}\}K_{1\text{-}4,6\text{-}9}$
GM → $\{u_6\}$: $\{K_{4,6}\}K_6$, $\{K_{1\text{-}4,6\text{-}9}\}K_{4,6}$, $\{K_{1\text{-}4,6\text{-}c}\}K_{1\text{-}4,6\text{-}9}$
GM → $\{u_1, u_2, u_3\}$: $\{K_{1\text{-}4,6\text{-}9}\}K_{123}$, $\{K_{1\text{-}4,6\text{-}c}\}K_{1\text{-}4,6\text{-}9}$
GM → $\{u_7, u_8, u_9\}$: $\{K_{1\text{-}4,6\text{-}9}\}K_{789}$, $\{K_{1\text{-}4,6\text{-}c}\}K_{1\text{-}4,6\text{-}9}$
GM → $\{u_a, u_b, u_c\}$: $\{K_{1\text{-}4,6\text{-}c}\}K_{abc}$