CSS322 – Quiz 3

Security and Cryptography, Semester 2, 2010

Prepared by Steven Gordon on 19 December 2010
CSS322Y10S2Q03, Steve/Courses/CSS322/Assessment/Quiz3.tex, r1573

Question 1 [5 marks]

Calculate the following. A calculator is *not allowed*. Show calculations/explanations.

(a) [$\phi(23)$ | $\phi(27)$ | $\phi(21)$ | $\phi(29)$] Answer: _____ [1.5 marks]

Answer. *23: prime number, therefore* $\phi(23) = 22$
27: relatively prime: 1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26; $\phi(23) = 18$
21: relatively prime: 1,2,4,5,8,10,11,13,16,17,19,20; $\phi(21) = 12$
29: prime number, therefore $\phi(29) = 28$

(b) [$\phi(25)$ | $\phi(31)$ | $\phi(37)$ | $\phi(26)$] Answer: _____ [1.5 marks]

Answer. *25: relatively prime: 1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24;* $\phi(25) = 20$
31: prime number, therefore $\phi(31) = 30$
37: prime number, therefore $\phi(37) = 36$
26: relatively prime: 1,3,5,7,9,11,15,17,19,21,23,25; $\phi(26) = 12$

(c) [$(40 \div 23) \bmod 80$ | $(16 \div 17) \bmod 42$ | $(20 \div 12) \bmod 59$ | $(30 \div 17) \bmod 67$] [2 marks]

Answer. $(40 \div 23) \bmod 80 : MI(23) = 7; (40 \times 7) \bmod 80 = 280 \bmod 80 = 40$
$(16 \div 17) \bmod 42 : MI(17) = 5; (16 \times 5) \bmod 42 = 80 \bmod 42 = 38$
$(20 \div 12) \bmod 59 : MI(12) = 5; (20 \times 5) \bmod 59 = 100 \bmod 59 = 41$
$(30 \div 17) \bmod 67 : MI(17) = 4; (30 \times 4) \bmod 67 = 120 \bmod 67 = 53$

(d) [$3^{32} \bmod 80$ | $5^{30} \bmod 124$ | $3^{28} \bmod 79$ | $4^{24} \bmod 62$] [Bonus: 2 marks]

Answer. $3^{32} \bmod 80 = 3^{4^8} \bmod 80 = 81^8 \bmod 80 = 1^8 \bmod 80 = 1$
$5^{30} \bmod 124 = 5^{3^10} \bmod 124 = 125^{10} \bmod 124 = 1^{10} \bmod 124 = 1$
$3^{28} \bmod 79 = 3^{4^7} \bmod 79 = 81^7 \bmod 79 = 2^7 \bmod 79 = 128 \bmod 79 = 49$
$4^{24} \bmod 62 = 4^{3^8} \bmod 62 = 64^8 \bmod 62 = 2^8 \bmod 62 = 256 \bmod 62 = 8$

Question 2 [2 marks]

Circle one or more of the following 5 algorithms that can be used in or as part of a PRNG:

Blum-Blum-Shub Triple DES RC4
Linear Congruential Generator AES in Counter Mode

Answer. *All of them can be used as PRNG*

Question 3 [3 marks]

Assume when encrypting 3-bit plaintext with a block cipher with key K, the following ciphertext is obtained:

P	C	P	C
000	110	100	000
001	001	101	011
010	111	110	101
011	010	111	100

The following ciphertext was encrypted with the above cipher with key K in counter mode (initial value 0): [100110000 | 101111010 | 010110001 | 001010100] What is the plaintext?

Answer: _____

Answer. *To decrypt in counter mode, encrypt the counter and XOR the result with the ciphertext. Encrypting three values of the counter produces:* `110`, `001` *and* `111`.

For ciphertext `100 110 000`, *XOR with* `110 001 111` *gives:* `010 111 111`.
For ciphertext `101 111 010`, *XOR with* `110 001 111` *gives:* `011 110 101`.
For ciphertext `010 110 001`, *XOR with* `110 001 111` *gives:* `100 111 110`.
For ciphertext `001 010 100`, *XOR with* `110 001 111` *gives:* `111 011 011`.