OLD DOMINION UNIVERSITY
CS 463

Homework 9

Madelene McFarlane

11/1/2023

#01096496

Question 1. [Points 7] RSA Signature Scheme (page 265 in the textbook): Given the following table describing the procedure for Alice to send a signed message with RSA signature to Bob, calculate the unknown entities and verify that Bob has received the correct message sent by Alice.

Alice	**Bob**
Chooses $p = 17, q = 47$	
Compute $n = p * q =$	
Compute $\phi(n) =$	
Choose $e = 11$	
Compute $d = e^{-1} \bmod \phi(n) =$	
Compute Public key $(e, n) =$ Private key $(d, n) =$	
Send Public key (e, n) to Bob:	Receives Alice's public key(e, n)
Message to send is $m = 6$	
Computes signatures s for $m = m^d \bmod n =$	
Send (m, s) to Bob:	Receives (m, s):
	Compute $m^{'} : s^e \bmod n =$
	Verifies $m = m^{'}$

CS 463 Madeleine McFarlane

HW9 = answer

(1)

Alice	Bob
$p = 17$, $q = 47$	
$n = 17 \cdot 47 = \boxed{799}$	
$\phi(n) = \phi(799) = \boxed{736}$	
$e = 11$	
$d = 11^{-1} \bmod 736 = \boxed{67}$	
$K_{pub} = (11, 799)$ $K_{priv} = (67, 799)$	
Sending	receveing
$m = 6$	
$s = 6^{67} \bmod 799 = \boxed{675}$	
Sending $(6, 675)$	receveing
	$m = 675^{11} \bmod 799 = \boxed{6}$
	$m\ 6 = m\ 6$ ✓

$\phi(799)$

$$\begin{array}{r|l} 47 & 799 \\ 47 & 17 \end{array} \qquad \begin{array}{r|l} 17 & 17 \\ 17 & 1 \end{array}$$

$\boxed{736}$

$799\left(1-\frac{1}{17}\right)\left(1-\frac{1}{47}\right)$

$799\left(\frac{17-1}{17}\right)\left(\frac{47-1}{47}\right)$

$17\left(\frac{17-1}{17}\right)(47-1)$

$1(17-1)(46)$

$1(16)(46)$

$11^{-1} \bmod 736$

$11 \cdot d = 1 \bmod 736$

$11 \cdot d \bmod 736 = 1$

$11 \cdot \boxed{67} \bmod 736$

$737 \bmod 736$

$1 = 1$

Question 2. [Points 7] Elgamal Signature Scheme (page 270-272): Given the following table describing the procedure for Alice to send a signed message with Elgamal signature to

Bob, calculate the unknown entities and verify that Bob has received the correct message sent by Alice.

Alice	**Bob**
Chooses $p = 17$	
Chooses a primitive element $\alpha = 7$	
Choose a random integer $d = 6$	
Compute $\beta = \alpha^d \bmod p =$	
Public key is $k_{pub} = (p, \alpha, \beta) =$ Private key is $k_{pr} = d =$	
Send Public Key $k_{pub} = (p, \alpha, \beta) =$ to Bob:	Recieves Alice' public key $k_{pub} = (p, \alpha, \beta) =$
Choose an ephemeral key $K_E = 7$	
Message to send is $m = 6$	
Computes signature (s, r) for m $r = \alpha^{K_E} \bmod p =$ Compute $K_E^{-1} \bmod (p-1) =$ $s = (m - d * r) * K_E^{-1} \bmod (p-1) =$	
Send $(m, (r, s))$ to Bob:	Recieves $(m, (r, s)) =$
	Compute $t = \beta^r * r^s \bmod p =$
	Verifies if $t = \alpha^m \bmod p =$

CS 463 HW9

Madeleine McFarlane

$\boxed{\ }$ = answer

(2)

Alice	Bob
$p = 17$	
$\alpha = 7$	
$d = 6$	
$\beta = 7^6 \bmod 17 = \boxed{9}$	
$K_{pub} = (17, 7, 9)$ $K_{pr} = 6$	
Send K_{pub}	Recieves K_{pub}
$K_E = 7$	
$m = 6$	
$r = 7^7 \bmod 17 = \boxed{12}$ $s = (6 - 6 \cdot 12) \cdot 7 = \boxed{2}$ (2, 12)	
Send (6, (12, 2))	Recieves
	$t = 9^{12} \cdot 12^2 \bmod 17 = \boxed{9}$ ✓
	$t = 7^6 \bmod 17 = \boxed{9}$ ✓

$7^6 \bmod 17$
$117{,}649 \bmod 17$
$\boxed{9}$

$7^7 \bmod 17$
$823{,}543 \bmod 17$
$\boxed{12}$

$7^{-1} \bmod 16$
$7 \cdot d \bmod 16 = 1$
$7 \cdot \underline{7} \bmod 16$
$49 \bmod 16$
$1 = 1$

$(6 - 6 \cdot 12) \cdot 7$
$(6 - 72) \cdot 7$
$-66 \cdot 7$
-462
+16
+16
+16 until positive
$\boxed{2}$

$9^{12} \cdot 12^2 \bmod 17$
$282{,}429{,}536{,}481 \cdot 144 \bmod 17$
$40{,}669{,}853{,}253{,}264 \bmod 17$
$\boxed{9}$

$7^6 \bmod 17$
$117{,}649 \bmod 17$
$\boxed{9}$

Question 3 [Points 6] Compute CBC-MAC (pages 325-326 in textbook) for a message of 24 bits, "789ABC" (in hexadecimal). Assume a block size of 8 bits with an IV=F5 (hexadecimal) and key = D4 (hexadecimal). Assume the encryption (and decryption) to be as follows: If plaintext is LT||RT and the key is LK||RK, where LC, RC, LT, and RT are each 4 bits, then ciphertext= LC||RC where LC=LK XOR RT; and RC = RK XOR LT; Plaintext and ciphertext are each 8 bits. Similarly, to decrypt ciphertext, we perform exactly the reverse operation where LT=RC XOR RK and RT = LC XOR LK.

(Hint: Divide the message into blocks of 8 bits each; XOR each block with the previous cipher output; then encrypt this with the key. For the first block, XOR it with IV. Details in pages 325-326 Ch.12 of the textbook)

CS 463 Madeleine McFarlane

HW9

: answer

F5 (IV) → 1111 0101

D4 (K) → 1101 0100

78 (x_1) → 0111 1000, 9A (x_2) → 1001 1010, BC (x_3) → 1011 1100

$y_1 = e_K(x_1 \oplus IV)$

$y_1 = e_{1101\,0100}\left((0111\,1000) \oplus (1111\,0101)\right)$

$y_1 = e_{1101\,0100}(1000\,1101)$

LT= 1000, RT= 1101, LK= 1101, RK= 0100

LC: 1101 ⊕ 1101 = 0000

RC= 0100 ⊕ 1000 = 1100

LC||RC = 0000 1100

$y_2 = e_{1101\,0100}(1001\,1010 \oplus 0000\,1100)$

$y_2 = e_{1101\,0100}(1001\,0110)$

LT= 1001, RT= 0110, LK= 1101, RK= 0100

LC: 1101 ⊕ 0110 = 1011

RC: 0100 ⊕ 1001 = 1101

LC||RC = 1011 1101

$y_3 = e_{1101\,0100}(1011\,1100 \oplus 1011\,1101)$

$y_3 = e_{1101\,0100}(0000\,0001)$

LT= 0000, RT= 0001, LK= 1101, RK= 0100

LC: 1101 ⊕ 0001 = 1100

RC: 0100 ⊕ 0000 = 0100

LC||RC = 1100 0100

$\boxed{1100\ 0100 = C4}$