Jevin Ale HW #10

Hi!
My notes & work
Can be found on
the next pages! :)

Question 3) F1

1) RSA signature Scheme

Alice	Bob
Choose $p=23, q=43$	
Compute $n=p \cdot q = 989$	
Compute $\varphi(n) = 924$	
Choose $e=17$	
Compute $d = e^{-1} \bmod \varphi(n) = 761$	
Public key: $(e,n) = (17,989)$	
Compute private key: $(d,n) = (761, 989)$	
Send public key (e,n) to Bob: $(17,989)$	Recieves Alice's public key (e,n): $(17,989)$
Message to send is $m=9$	
Compute sigs s for $m: m^d \bmod n = 220$	
Send (m,s) to Bob $(9,220)$	Recieves (m,s): $(9,220)$
	Compute $m': s^e \bmod n = 9$
	Verifies if $m=m'$ $9=9$ ✓

2) ElGamal Signature Scheme

Alice	Bob
choose $p=17$	
Choose a prim element $a=11$	
$d=7$	
Compute $\beta = a^d \bmod p = 6$	
public key $= (p,a,b) = (17,11,6)$; $d=7=k_{pr}$	
Send $k_{pub} = (p,a,\beta)$ to bob! $(17,11,6)$	Recieves Alice k_{pub} $(17,11,6)$
Choose Ephemeral $kE=5$	
$m=9$	
$r = a^{kE} \bmod p = 10$; $kE^{-1} \bmod (p-1) = 13$;	
$s = (m - d \cdot r) kE^{-1} \bmod (p-1) = 7$	
Send $(m,(r,s))$ to Bob $(9,(10,7))$	Recieve $(m,(r,s)) = (9,(10,7))$
	$t = \beta^r \cdot r^s \bmod p = 1$
	$t = \alpha^m \bmod p = 1$ ✓

Jenia ali zelv 10

1) step 1 $n = p \cdot q$

$p = 23, q = 43 \Rightarrow n = 23 \times 43 = 989$

step 2 $\phi(n)$

$\phi(n) = (p-1)(q-1) = (23-1)(43-1) = 22 \times 42 = 924$

step 3 Choose $e = 17$

$\gcd(e, \phi(n)) = 1$? $\Rightarrow \gcd(17, 924) = 1$ ✓

$e = 17$ ✓

step 4 Compute $d = e^{-1} \bmod \phi(n)$, mod inverse of 17 modulo 924:

Extended euclidean alg: $17d \equiv 1 \bmod 924$

$924 = 54 \cdot 17 + 6 \Rightarrow 17 = 2 \cdot 6 + 5 \Rightarrow$

$6 = 1 \cdot 5 + 1 \Rightarrow 5 \equiv 5 \cdot 1 \bmod 10 \Rightarrow$ ✓

Substitute coeff.

$1 = 6 - 1 \cdot 5 \Rightarrow 6 - 1(17 - 2 \cdot 6) \Rightarrow$

$3 \cdot 6 - 1 \cdot 17 \Rightarrow 3(924 - 54 \cdot 17) - 1 \cdot 17 \Rightarrow 3 \cdot 924 - 163 \cdot 17$ ✓

$\Rightarrow 1 = 3 \cdot 924 - 163 \cdot 17 \Rightarrow$

$d = 761 \bmod 924$

step 5

public key: $(e, n) = (17, 989)$

private key: $(d, n) = (761, 989)$

step 6 $m = 9$

$s = m^d \bmod n = 9^{761} \bmod 989 \Rightarrow$ fast exponentiation using python

$s = 220$ pow(9, 761, 989) = 220

Step 7

Bob verifies sig $(m=9, s=220)$

He computes: $m' = s^e \bmod n = 220^{17} \bmod 989 \Rightarrow$

pow(220, 17, 989) = 9 $\Rightarrow$ $m' = 9$ ✓

---

2) ElGamal Sig Scheme

Step 1

$\beta = a^d \bmod p$, $a=11, d=7, p=17 \Rightarrow 11^7 \bmod 17 \Rightarrow$

fast exponentiation python $\Rightarrow$ pow(11, 7, 17) = 6

Step 2 Public privacy

public: $(p, a, \beta) = (17, 11, 6)$

private: $d = 7$

Step 3

$r = a^{kE} \bmod p$, $kE=5, a=11, p=17 \Rightarrow r = 11^5 \bmod 17 = 10 \Rightarrow$

pow(11, 5, 17) = 10

Step 4

$kE^{-1} \bmod (p-1) \Rightarrow kE^{-1} \bmod (17-1) = 5^{-1} \bmod 16 \Rightarrow \gcd($

$5, 16): 16 = 3 \cdot 5 + 1 \Rightarrow 1 = 16 - 3 \cdot 5 \Rightarrow -3 \cdot 5 = 1 \bmod 16 \Rightarrow$

$kE^{-1} = 13$

Step 5

$s = (m - d \cdot r) \cdot kE^{-1} \bmod (p-1)$; $m=9, d=7, r=10, kE^{-1}=13$,

$p-1 = 16 \Rightarrow s = (9 - 7 \cdot 10) \cdot 13 \bmod 16 = (9 - 70) \cdot 13 \bmod 16 = (-61) \cdot 13 \bmod 16$

$-61 \bmod 16 = -61 + 64 = 3 \Rightarrow s = 3 \cdot 13 \bmod 16 = 39 \bmod 16 = 7$

Step 6: Signature $(r,s) = (10,7)$

Alice sends $(m=9, (r=10, s=7))$

Step 7: Bob verify

$L = r \cdot r^s \bmod p = 6^{10} \cdot 10^7 \bmod 17 \Rightarrow pow(6,10,17) = 15$

$pow(10,7,17) = 8$

$t = (15 \cdot 8) \bmod 17 = 120 \bmod 17 = 1$ ✓

$m \bmod p = 11^9 \bmod 17 \Rightarrow pow(11,9,17) = 1$ ✓

$t = 1,\ m \bmod p = 1 \Rightarrow t = m \Rightarrow$ Sig valid ✓

3) Comp table

Step	in (Hex	Xor w/	Xor Result (Binary	LT	RT
1	A1: 10100001	IV: D3 = 11010011	01110010	0111	0010
2	A2: 10100010	Prev: C3 = 11000011	01100001	0110	0001
3	A3: 10100011	Prev: F2 = 11110010	01010001	0101	0001

	LCount RT	RC = RH ⊕ LT	Ciphertext Binary	Ciphertext Hex
1	1100	0011	11000011	C3
2	1111	0010	11110010	F2
3	1111	0001	11110001	F1