Name:
Student I.D:

Quiz 2

SOEN321: Fall 2020

IT IS REQUIRED TO SHOW THE DETAILS OF ALL OF YOUR CALCULATIONS

Prob. 1 Suppose that users Alice and Bob carry out the 3-pass Diffie-Hellman protocol with p = 113. Suppose that Alice chooses $a_1 = 17$ and Bob chooses $b_1 = 23$. If Alice wants to send the secret message m=5 to Bob, show all the messages exchanged between Alice and Bob

Prob. 2 Consider an RSA system with n=221, e1=37 and e2=55. Suppose the same message m was sent to the two users above and the attacker observed the ciphertext c_1=124 and c_2=45. Show how the attacker can recover the message.

Prob. 3 Consider a Rabin cryptosystem where the public key of Alice is n_a=437 and the public key of Bob is n_b= 869. If Charlie sends the same message to both Alice and Bob with c_a=100 and c_b=597. Show how Eve can determine this message without factoring n_a or n_b. Show all the details of your computations.

Quiz October 26 2020

②

1) 3 pass diffie hellman

$p=113 \quad a_1=17 \quad b_1=23 \quad m=5$

$a_2 = a_1^{-1} \bmod (p-1)$
$= 17^{-1} \bmod 112$
gcd(17, 112)
$112 = 6 \cdot 17 + 10$
$17 = 1 \cdot 10 + 7$
$10 = 1 \cdot 7 + 3$
$7 = 2 \cdot 3 + 1$
extended
$1 = 7 - 2 \cdot 3$
$1 = 7 - 2(10-7)$
$1 = 7 - 2 \cdot 10 + 2 \cdot 7$
$1 = 3 \cdot 7 - 2 \cdot 10$
$1 = 3(17-10) - 2 \cdot 10$
$1 = 3 \cdot 17 - 3 \cdot 10 - 2 \cdot 10$
$1 = 3 \cdot 17 - 5 \cdot 10$
$1 = 3 \cdot 17 - 5(112 - 6 \cdot 17) \bmod 112$
$1 = 3 \cdot 17 + 30 \cdot 17$
$1 = \boxed{33} \cdot 17 \bmod 112$
$\boxed{a_2 = 33}$

$b_2 = b_1^{-1} \bmod (p-1)$
$= 23^{-1} \bmod 112$
gcd(23, 112)
$112 = 4 \cdot 23 + 20$
$23 = 1 \cdot 20 + 3$
$20 = 6 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
extended
$1 = 3 - 2$
$1 = 3 - (20 - 6 \cdot 3)$
$1 = 3 - 20 + 6 \cdot 3$
$1 = 7 \cdot 3 - 20$
$1 = 7(23 - 20) - 20$
$1 = 7 \cdot 23 - 7 \cdot 20 - 20$
$1 = 7 \cdot 23 - 8 \cdot 20$
$1 = 7 \cdot 23 - 8 \cdot (112 - 4 \cdot 23) \bmod 112$
$1 = 7 \cdot 23 + 32 \cdot 23$
$1 = \boxed{39} \cdot 23 \bmod 112$
$b_2 = 39$

Alice ① $K^{a_1} \bmod p = \boxed{37}$ Bob
② $K^{a_1 b_1} \bmod p = \boxed{45}$
③ $K^{b_1} \bmod p = \boxed{17}$
$(K^{a_1 b_1})^{a_2}$
Bob decrypts $39 \bmod 113$ with 17
$= 5$

① $5^{17} \bmod 113$
$\to 10001$
$5^1 = 5 \bmod 113$ 1
$5^2 = 25 \bmod 113$ 0
$5^4 = 60 \bmod 113$ 0
$5^8 = 97 \bmod 113$ 0
$5^{16} = 30 \bmod 113$ 1
$= 5 \cdot 30 \bmod 113$
$= \boxed{37} \bmod 113$

② $37^{23} \bmod 113$
$\to 10111$
$37^1 = 37 \bmod 113$ 1
$37^2 = 13 \bmod 113$ 1
$37^4 = 56 \bmod 113$ 1
$37^8 = 85 \bmod 113$ 0
$37^{16} = 106 \bmod 113$ 1
$= 37 \cdot 13 \cdot 56 \cdot 106 \bmod 113$
$= \boxed{45} \bmod 113$

③ $45^{33} \bmod 113$
$\to 100001$
$45^1 = 45 \bmod 113$ 1
$45^2 = 109 \bmod 113$ 0
$45^4 = 81 \bmod 113$ 0
~~$45^8 = 7 \bmod 113$~~ 0
$45^{16} = 49 \bmod 113$ 0
$45^{32} = 28 \bmod 113$ 1
$= 45 \cdot 28 \bmod 113$
$= \boxed{17} \bmod 113$

45^{a_2}

② $n = 221$ $e_1 = 37$ $e_2 = 55$ $c_1 = 124$ $c_2 = 45$

gcd(e_1, e_2)

$55 = 1 \cdot 37 + 18$

$37 = 2 \cdot 18 + 1$

ext

$1 = 37 - 2 \cdot 18$

$1 = 37 - 2 \cdot (55 - 37)$

$1 = 37 - 2 \cdot 55 + 2 \cdot 37$

$1 = 3 \cdot 37 - 2 \cdot 55$

$a_1 e_1 \quad a_2 e_2$

$m = c_1^{a_1} \cdot c_2^{a_2} \bmod n$

$m = 124^3 \cdot 45^{-2} \bmod 221$

$= 57 \cdot (167)^2 \bmod 221$

$= 57 \cdot 27889 \bmod 221$

$= 57 \cdot 43 \bmod 221$

$m = 20 \bmod 221$

$124^3 \bmod 221$

$= 11$

$124^1 = 124 \bmod 221$

$124^2 = 127 \bmod 221$

$= 124 \cdot 127 \bmod 221$

$= 57 \bmod 221$

$45^{-2} = (45^{-1})^2$

$45^{-1} \bmod 221$

$221 = 4 \cdot 45 + 41$

$45 = 1 \cdot 41 + 4$

$41 = 10 \cdot 4 + 1$

$1 = 41 - 10 \cdot 4$

$1 = 41 - 10(45 - 41)$

$= 41 - 10 \cdot 45 + 10 \cdot 41$

$= 11 \cdot 41 - 10 \cdot 45$

$= 11(221 - 4 \cdot 45) - 10 \cdot 45 \bmod 221$

$= 44 \cdot 45 - 10 \cdot 45$

$= -54 \cdot 45 \bmod 221$

$= 167 \bmod 221$

(3)

Rabin $n_a = 437$ $c_a = 100$

$n_b = 869$ $c_b = 597$

$c = m^2 \bmod n$

$m^2 = c \bmod n$

$m^2 = 100 \bmod 437$ CRT

$m^2 = 597 \bmod 869$

$m^2 = 100(869) \cdot [869^{-1} \bmod 437]$ ①

$+ 597(437) \cdot [437^{-1} \bmod 869]$ ② $\bmod (437 \cdot 869)$

$= 100(869)(262)$

$+ 597(437)(348) \bmod (379\,753)$

$= 22\,767\,800 + 90\,789\,372 \bmod (379\,753)$

$= 362\,373 + 28\,405 \bmod (379\,753)$

$= 390\,778 \bmod 379\,753$

$m^2 = 11025$ $m = 105$

② $437^{-1} \bmod 869$

$869 = 1 \cdot 437 + 432$

$437 = 1 \cdot 432 + 5$

$432 = 86 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2 = 5 - 2(432 - 86 \cdot 5)$

$= 5 - 2 \cdot 432 + 172 \cdot 5$

$1 = 173 \cdot 5 - 2 \cdot 432$

$1 = 173(437 - 432) - 2 \cdot 432$

$1 = 173 \cdot 437 - 173 \cdot 432 - 2 \cdot 432$

$1 = 173 \cdot 437 - 175 \cdot 432$

$1 = 173 \cdot 437 - 175(869 - 437)$

$1 = 173 \cdot 437 + 175 \cdot 437$

$1 = 348 \cdot 437 \bmod 869$

① $869^{-1} \bmod 437$

$[869 \bmod 437]^{-1} \bmod 437$

$432^{-1} \bmod 437$

gcd

$437 = 1 \cdot 432 + 5$

$432 = 86 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2$

$1 = 5 - 2(432 - 86 \cdot 5)$

$1 = 5 - 2 \cdot 432 + 172 \cdot 5$

$1 = 173 \cdot 5 - 2 \cdot 432$

$1 = 173(437 - 432) - 2 \cdot 432$

$= 173 \cdot 432 - 2 \cdot 432$

$= -175 \cdot 432 \bmod 437$

$= 262 \cdot 432 \bmod 437$