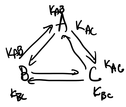
Assignment 3

Wednesday, November 17, 2021 8:30 PM

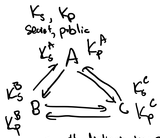
1. Symmetric key cryptosystem



$\frac{(m-1)m}{2} \rightarrow m=1000$

distinct keys: $\frac{(999)(1000)}{2} = 499500$ distinct keys

Public key cryptosystem:



so # distinct keys is $2m$
if $m=1000 \rightarrow$ # of distinct keys $=2000$

2. Programming

3.

a. $x \equiv 12 \bmod 25$ $a_1=12$ $a_2=9$ $a_3=23$
$x \equiv 9 \bmod 26$ $m_1=25$ $m_2=26$ $m_3=27$
$x \equiv 23 \bmod 27$

$M_1 = \frac{M}{m_1} = \frac{25 \cdot 26 \cdot 27}{25} = 702$

$M_2 = \frac{M}{m_2} = \frac{25 \cdot 26 \cdot 27}{26} = 675$

$M_3 = \frac{M}{m_3} = \frac{25 \cdot 26 \cdot 27}{27} = 650$

$702x_1 \equiv 1 \bmod 25 \rightarrow x_1 = 13$

$675x_2 \equiv 1 \bmod 26 \rightarrow x_2 = 25$

$650x_3 \equiv 1 \bmod 27 \rightarrow x_3 = 14$

$x = a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod M$

$x = 470687 \bmod 17550 = 14387 \bmod 17550$

b. $13x \equiv 4 \bmod 99$

$15x \equiv 56 \bmod 101$

$x_1 = 13 \pmod{99}$, $x_2 = 15 \bmod 101$

$13x_1 = 99z_1 + 1 = 91z_1 + (8z_1 + 1)$

$z_1 = 8 \rightarrow 91(8) + (8(8)+1) = 13x_1 \Rightarrow x_1 = 61$

$15x_2 \equiv 1 \bmod 101$

$15x_2 = 101z_2 + 1 = 90z_2 + (11z_2 + 1)$

$z_2 = 4 \rightarrow 15x_2 = 90(4) + (11(4)+1) = 27$

$x = 299 \bmod 99 \Rightarrow x = 46 \bmod 99$
$x = 1512 \bmod 101 \Rightarrow x = 98 \bmod 101$

$a_1 = 46$ $a_2 = 98$ $m_1 = 99$ $m_2 = 101$, $M = 99 \cdot 101 = 9999$

$24y_1 = 99z_1 + 1 = 98z_1 + (1 + z_1) \rightarrow y_1 = 50$

$99y_2 = 101z_2 + 1 \rightarrow 99y_2 = 99z_2 + (2z_2 + 1) \rightarrow y_2 = 50$

$x = a_1 \cdot M_1y_1 + a_2M_2 + y_2 \pmod M$

$x = 46 \cdot 101 \cdot 50 + 98 \cdot 99 \cdot 50 \pmod{9999} = 7471 \pmod{9999}$

4a. An eavesdropper "E" can create a table using the public key that correlates between the plaintext and the ciphertext. Because with only 25 characters, through brute-force, E would easily decrypt the message

b. Programming

5. $516107^2 = 7 \bmod 642401$ $187722^2 = 2^2 \cdot 7 \bmod 642401$

$516107^2 \cdot 187722^2 = 7^2 2^2 \bmod 642401$

$= 14^2 \bmod 642401$

$289038^2 - 14^2 = 0 \bmod 642401$

$(289038 - 14)(289038 + 14) = 11$

$\gcd(289052, 642401)$

$642401 = 289052(2) + 64297$

$289052 = 64297(4) + 31864$

$64297 = 31864(2) + 569$

$31864 = 569(56) + 0$

$C_3 \frac{642401}{569} = 1129$ [569, 1129]

need 2c
7
9

6a. Steps:

1. multiply the first three equations together
2. use euclidean algorithm and compute gcd of result pair
3. With first factor, divide with 22882333 to get other factor

b. Programming

7. Programming

8. $y_1 = \alpha^{k_1} \bmod p$

$y_1 = m_1\beta^{k_1} \bmod p = m_1\alpha^{ak_1} \bmod p$

$y_3 = \alpha^{k_2} \bmod p$

$y_4 = m\beta^{k_2} \bmod p = m_2\alpha^{ak_2} \bmod p$

$P_{dk}(C) = y_2y_4[(y_1y_3)^a]^{-1} \bmod p$

$= m_1\alpha^{ak_1}m_2\alpha^{ak_2}[(\alpha^{k_1}\alpha^{k_2})^a]^{-1} \bmod p$

$= m_1m_2\alpha^{a(k_1+k_2)}[\alpha^{a(k_1+k_2)}]^{-1} \bmod p$

$= \boxed{m_1m_2 \pmod p}$

9. Programming