Intermediate Math Circles
April 2, 2014
Cryptography III - Solutions

Problem Set 1:

1. What is the reminder when 8^{38} is divided by 3?

   $8 \equiv 2 \pmod 3$
   $8^2 \equiv 2^2 \equiv 1 \pmod 3$
   $\therefore 8^{38} \equiv (8^2)^{19} \equiv 1^{19} \equiv 1 \pmod 3$

   OR

   $8 \equiv -1 \pmod 3$
   $8^{38} \equiv (-1)^{38} \equiv 1 \pmod 3$

2. Determine the remainder when 16^{47} is divided by 6.

   Reduce $16^{47} \pmod 6$
   $16 \equiv 4 \pmod 6$
   $16^2 \equiv 4^2 \equiv 16 \equiv 4 \pmod 6$
   $16^4 \equiv 4^2 \equiv 4 \pmod 6$
   $16^8 \equiv 4^2 \equiv 4 \pmod 6$
   $16^{16} \equiv 4 \pmod 6$
   $16^{32} \equiv 4 \pmod 6$

   $47 = 32 + 8 + 4 + 2 + 1$

   $\therefore 16^{47} \equiv 16^{32}16^8 16^4 16^2 16 \pmod 6$
   $\equiv \underline{4 \cdot 4} \cdot \underline{4 \cdot 4} \cdot 4 \pmod 6$
   $\equiv \underline{4 \cdot 4} \cdot 4 \pmod 6$
   $\equiv 4 \cdot 4 \pmod 6$
   $\equiv 4 \pmod 6$

3. If today is a Wednesday, what day of the week will it be 2^{100} days from now?

   Reduce $2^{100} (\text{mod} 7)$
   $2^3 \equiv 8 \equiv 1 (\text{mod } 7)$
   $100 = 3 \cdot 33 + 1$
   $\therefore 2^{100} = (2^3)^{33} \cdot 2 \equiv 1^{33} \cdot 2 (\text{mod } 7) \equiv 2 (\text{mod} 7)$
   $\therefore$ It is a Friday

4. Is $5^{21} + 8^{41}$ divisible by 7?

   First reduce $5^{21} (\text{mod} 7)$ and $8^{41} (\text{mod} 7)$

   $5^2 \equiv 25 \equiv 4 (\text{mod} 7)$
   $5^4 \equiv (5^2)^2 \equiv 4^2 \equiv 16 \equiv 2 (\text{mod} 7)$
   $5^8 \equiv 2^2 \equiv 4 (\text{mod} 7)$
   $5^{16} \equiv 4^2 \equiv 16 \equiv 2 (\text{mod} 7)$
   $\therefore 5^{21} \equiv 5^{16} \cdot 5^4 \cdot 5 \equiv 2 \cdot 2 \cdot 5 \equiv 20 \equiv 6 (\text{mod} 7)$

   $8 \equiv 1 (\text{mod} 7)$
   $\therefore 8^{41} \equiv 1^{41} \equiv 1 (\text{mod} 7)$

   $\therefore 5^{21} + 8^{41} \equiv 6 + 1 \equiv 7 \equiv 0 (\text{mod} 7)$

   So 7 divides $(5^{21} + 8^{41}) - 0$
   i.e. $5^{21} + 8^{41}$ is divisible by 7

5. Reduce 25^{23} modulo 143.

   Use Square & Multiply Algorithm:

   $25^2 \equiv 625 \equiv 53 (\text{mod} 143)$
   $25^4 \equiv 53^2 \equiv 2809 \equiv 92 (\text{mod} 143)$
   $25^8 \equiv 92^2 \equiv 8464 \equiv 27 (\text{mod} 143)$
   $25^{16} \equiv 27^2 \equiv 729 \equiv 14 (\text{mod} 143)$

   $\therefore 25^{23} \equiv 25^{16} 25^4 25^2 25^1 (\text{mod} 143)$
   $\equiv 14 \cdot 92 \cdot 53 \cdot 25 (\text{mod} 143)$
   $\equiv 1288 \cdot 1325 (\text{mod} 143)$
   $\equiv 1 \cdot 38 (\text{mod} 143)$
   $\equiv 38 (\text{mod} 143)$

6. Reduce 38^{47} modulo 143.

   Use Square & Multiply Algorithm:

   $38^2 \equiv 1444 \equiv 14 (\text{mod} 143)$
   $38^4 \equiv 14^2 \equiv 53 (\text{mod} 143)$
   $38^8 \equiv 53^2 \equiv 2809 \equiv 92 (\text{mod} 143)$
   $38^{16} \equiv 92^2 \equiv 8464 \equiv 27 (\text{mod} 143)$
   $38^{32} \equiv 27^2 \equiv 729 \equiv 14 (\text{mod} 143)$

   $\therefore 38^{47} \equiv 38^{32}38^8 38^4 38^2 38^1 (\text{mod} 143)$
   $\equiv \underline{14 \cdot 92} \cdot \underline{53 \cdot 14} \cdot 38 (\text{mod} 143)$
   $\equiv 1288 \cdot 742 \cdot 38 (\text{mod} 143)$
   $\equiv 1 \cdot 27 \cdot 38 (\text{mod} 143)$
   $\equiv 1026 (\text{mod} 143)$
   $\equiv 25 (\text{mod} 143)$

Problem Set 2:

1. In last week's Math Circle, Problem Set 2, #1, we set up the RSA key pair: public key $(e, n) = (23, 143)$, private key $(d, n) = (47, 143)$

   a) Encrypt the plaintext $M = 13$ (use the public key)

   Reduce $13^{23} (\text{mod} 143)$

   $13^2 \equiv 169 \equiv 26 (\text{mod} 143)$
   $13^4 \equiv 26^2 \equiv 676 \equiv 104 (\text{mod} 143)$
   $13^8 \equiv 104^2 \equiv 10816 \equiv 91 (\text{mod} 143)$
   $13^{16} \equiv 91^2 \equiv 8281 \equiv 130 (\text{mod} 143)$

   $\therefore 13^{23} \equiv 13^{16}13^4 13^2 13^1 (\text{mod} 143)$
   $\equiv 130 \cdot 104 \cdot 26 \cdot 13 (\text{mod} 143)$
   $\equiv 13520 \cdot 338 (\text{mod} 143)$
   $\equiv 78 \cdot 52 (\text{mod} 143)$
   $\equiv 52 (\text{mod} 143)$

   $\therefore C = 52$

b) Decrypt the ciphertext $C = 52$ (use the private key)

Reduce $52^{47} (\text{mod} 143)$

$52^2 \equiv 2704 \equiv 130 (\text{mod} 143)$
$52^4 \equiv 130^2 \equiv 16900 \equiv 26 (\text{mod} 143)$
$52^8 \equiv 26^2 \equiv 676 \equiv 104 (\text{mod} 143)$
$52^{16} \equiv 104^2 \equiv 10816 \equiv 91 (\text{mod} 143)$
$52^{32} \equiv 91^2 \equiv 8281 \equiv 130 (\text{mod} 143)$

$\therefore 52^{47} \equiv 52^{32}52^8 52^4 52^2 52^1 (\text{mod} 143)$
$\equiv \underline{130 \cdot 104} \cdot \underline{26 \cdot 130} \cdot 52 (\text{mod} 143)$
$\equiv 13520 \cdot 3380 \cdot 52 (\text{mod} 143)$
$\equiv 78 \cdot 91 \cdot 52 (\text{mod} 143)$
$\equiv 13 (\text{mod} 143)$

$\therefore M = 13$

2. In last week's Math Circle, Problem Set 2, #2, we set up the RSA key pair: public key $(e, n) = (19, 115)$ private key $(d, n) = (51, 115)$

a) Encrypt the plaintext $M = 13$ (use the public key)

Reduce $M^e (\text{mod n})$ OR $13^{19} (\text{mod} 115)$

$13^2 \equiv 169 \equiv 54 (\text{mod} 115)$
$13^4 \equiv 54^2 \equiv 2916 \equiv 41 (\text{mod} 115)$
$13^8 \equiv 41^2 \equiv 1681 \equiv 71 (\text{mod} 115)$
$13^{16} \equiv 71^2 \equiv 5041 \equiv 96 (\text{mod} 115)$

$\therefore 13^{19} \equiv 13^{16}13^2 13^1 (\text{mod} 115)$
$\equiv 96 \cdot \underline{54 \cdot 13} (\text{mod} 115)$
$\equiv 96 \cdot 702 (\text{mod} 115)$
$\equiv 96 \cdot 12 (\text{mod} 115)$
$\equiv 1152 \equiv 2 (\text{mod} 115)$

$\therefore C = 2$

b) Decrypt the ciphertext $C = 2$ (use the private key)

Reduce $C^d \pmod{n}$ OR $2^{51} \pmod{115}$

$2^2 \equiv 4 \pmod{115}$
$2^4 \equiv 16 \pmod{115}$
$2^8 \equiv 16^2 \equiv 256 \equiv 26 \pmod{115}$
$2^{16} \equiv 26^2 \equiv 676 \equiv 101 \pmod{115}$
$2^{32} \equiv 101^2 \equiv 10201 \equiv 81 \pmod{115}$

$\therefore 2^{51} \equiv 2^{32}2^{16}2^2 2^1 \pmod{115}$
$\equiv \underline{81 \cdot 101} \cdot \underline{4 \cdot 2} \pmod{115}$
$\equiv 162 \cdot 404 \pmod{115}$
$\equiv 47 \cdot 59 \pmod{115}$
$\equiv 2773 \equiv 13 \pmod{115}$

$\therefore M = 13$

3. In last week's Math Circle, Problem Set 2, #3, we set up the RSA key pair: public key $(e, n) = (29, 253)$ private key $(d, n) = (129, 253)$

a) Encrypt the plaintext $M = 4$ (use the public key)

Reduce $4^{29} \pmod{253}$

$4^2 \equiv 16 \pmod{253}$
$4^4 \equiv 16^2 \equiv 256 \equiv 3 \pmod{253}$
$4^8 \equiv 3^2 \equiv 9 \pmod{253}$
$4^{16} \equiv 9^2 \equiv 81 \pmod{253}$

$\therefore 4^{29} \equiv 4^{16}4^8 4^4 4^1 \pmod{253}$
$\equiv \underline{81 \cdot 9} \cdot \underline{3 \cdot 4} \pmod{253}$
$\equiv 729 \cdot 12 \pmod{253}$
$\equiv 223 \cdot 12 \pmod{253}$
$\equiv 2676 \equiv 146 \pmod{253}$

$\therefore C = 146$

b) Decrypt the ciphertext $C = 146$ (use the private key)

Reduce $146^{129} (\text{mod} 253)$

$146^2 \equiv 21316 \equiv 64 (\text{mod} 253)$
$146^4 \equiv 64^2 \equiv 4096 \equiv 48 (\text{mod} 253)$
$146^8 \equiv 48^2 \equiv 2304 \equiv 27 (\text{mod} 253)$
$146^{16} \equiv 27^2 \equiv 729 \equiv 223 (\text{mod} 253)$
$146^{32} \equiv 223^2 \equiv 49729 \equiv 141 (\text{mod} 253)$
$146^{64} \equiv 141^2 \equiv 19881 \equiv 147 (\text{mod} 253)$
$146^{128} \equiv 147^2 \equiv 21609 \equiv 104 (\text{mod} 253)$

$\therefore 146^{129} \equiv 146^{128} 146^1 (\text{mod} 253)$
$\equiv 104 \cdot 146 (\text{mod} 253)$
$\equiv 15184 \equiv 4 (\text{mod} 253)$

$\therefore M = 4$