College of Computer and Information Science

Northeastern University

CSG252: Cryptography and Communication Security

Fall 2005

Problem Set 6 - Solutions

Prepared by Tim Morgan

Problem 1 [20 points]:

$x = 7471$

Problem 2 [10 points]:

$2^{48} mod\ 97 = 1$

$3^{48} mod\ 97 = 1$

$4^{48} mod\ 97 = 1$

However, $5^{48} mod\ 97 = 96$ and $5^{32} mod\ 97 = 35$, therefore the smallest primitive root modulo 97 is 5.

Problem 3 [20 points]:

Suppose $x \not\equiv 0\ (mod\ p)$. Then for some integer $k > 0$, it holds that:

$$x^{ab} = x^{1+k(p-1)(q-1)} \equiv x \times x^{k(p-1)(q-1)} \equiv x\ (mod\ p)$$

If $x \equiv 0\ (mod\ p)$, then $x^{ab} \equiv x \equiv 0\ (mod\ p)$. Therefore $x^{ab} \equiv x\ (mod\ p)$ for any $x \epsilon Z_p$. Similarly, $x^{ab} \equiv x\ (mod\ p)$ for any $x \epsilon Z_p$. Now, applying the hint, $x^{ab} \equiv x\ (mod\ n)$for any $x \epsilon Z_n$.

Problem 4 [10 points]:

The first plaintext was encrypted using the values $n = 18923 = 127 \times 149$ and $b = 1261$. Hence $\phi(n) = 126 \times 148 = 18648$ and $a = 1261^{-1} mod\ 18648 = 5797$.

The first ciphertext element, $y = 12423$, is decrypted to $x = 5438$. We convert this to three letters as follows:

$5438\ mod\ 26 = 4$
$(5438 - 4)/26 = 209$
$209\ mod\ 26 = 1$
$(209 - 1)/26 = 8$
$8\ mod\ 26 = 8$

Therefore, the triple (8,1,4) correspondes to the three letters (*i, b, e*). The first plaintext was taken from "The Diary of Samuel Marchbanks" by Robertson Davies and is as follows:

> I became involved in an argument about modern painting, a subject upon which I am spectacularly ill-informed. However, many of my friends can become heated and even violent on the subject, and I enjoy their wrangles in a modest way. I am an artist myself and I have some sympathy with the abstractionists, although I have gone beyond them in my own approach to art. I am a lumpist. Two or three decades ago it was quite fashionable to be a cubist and to draw everything in cubes. Then there was a revolt by the vorticists who drew everything in whirls. We now have the abstractionists who paint everything in a very abstracted manner, but my own small works done on my telephone pad are composed of carefully shaded, strangely shaped lumps with traces of cubism, vorticism, and abstractionism in them. For those who possess the seeing eye, as a lumpist, I stand alone.

The second plaintext was encrypted using the values $n = 31313 = 173 \times 181$ and $b = 4913$. Hence, $\phi(n) = 172 \times 180 = 30960$ and $a = 4913^{-1}\ mod\ 30960 = 6497$. The second plaintext was taken from "Lake Wobegon Days" by Garrison Keillor and is as follows:

> Lake Wobegon is mostly poor sandy soil, and every spring the earth heaves up a new crop of rocks. Piles of rocks ten feet high in the corners of fields, picked by generations of us, monuments to our industry. Our ancestors chose the place, tired from their long journey, sad for having left the motherland behind, and this place reminded them of there, so they settled here, forgetting that they had left there because the land wasn't so good. So the new life turned out to be a lot like the old, except the winters are worse.

Problem 5 [10 points]:

Choose a random x_0 and compute $y_0 = e_K(x_0)$. Define $\hat{y} = y_0 \cdot y\ mod\ n$, and obtain the decryption $\hat{x} = d_K(\hat{y})$. Then compute $x = \hat{x} \cdot x_0^{-1} mod\ n$.

Problem 6 [10 points]:

The first ciphertext element, (3781, 14409), is decrypted to the plaintext element:

$$x = 14409((3781)^{7899})^{-1} \ mod \ 31847 = 12354$$

$x = 12354$ encodes the triple (18, 7, 4), which correstonds to the three letters (*s, h, e*).

Problem 7 [20 points]:

(a)

$$\begin{aligned} x &\equiv M_p \cdot q \cdot x_p \ (mod \ p) \\ &\equiv q^{-1} \cdot q \cdot x_p \ (mod \ p) \\ &\equiv x_p \ (mod \ p) \\ &\equiv y^{d_p} \ (mod \ p) \\ &\equiv y^d \ (mod \ p) \end{aligned}$$

because $d_p \equiv d \ (mod \ p-1)$. Similarly, $x \equiv y^d \ (mod \ q)$.

Therefore $x \equiv y^d \ (mod \ n)$.

(b)

If $d = 1234577$, then:

$d_p = 907$
$d_q = 1345$
$M_p = 777$
$M_q = 973.$

(c)

$x_p = 242$
$x_q = 1087$
$x = 1443247$