Cryptology - Week 4 worksheet

These exercises are to aid your learning on the lecture material from week 4. They build up in difficulty, and a slightly harder version of the final *non-starred* exercise will be on the exam. If you have handed in your homework sheet and understood any feedback given, that should be sufficient revision for the relevant exam question.

1. (a) Using double-and-add, compute $69 \cdot 73 \pmod{1000}$. Write out your steps and compute the number of additions required.
Hint: the binary expansion of 69 is 1000101.

$p = 73, \quad q = 69, \quad \lambda = \text{length}(1000101) - 1 = 6$

<u>Double</u>: $2^0 \cdot 73 = 73$

$$\left.\begin{aligned}
2^1 \cdot 73 &= 73 + 73 = 146 \\
2^2 \cdot 73 &= 146 + 146 = 292 \\
2^3 \cdot 73 &= 292 + 292 = 584 \\
2^4 \cdot 73 &= 584 + 584 = 1168 \\
2^5 \cdot 73 &= 1168 + 1168 = 2336 \\
2^6 \cdot 73 &= 2336 + 2336 = 4672
\end{aligned}\right\} \text{6 additions}$$

✓

<u>Add</u>: q has nonzero digits at $i = 0, 2,$ and 6.

Thus we compute

$$(2^0 \cdot 73) + (2^2 \cdot 73) + (2^6 \cdot 73)$$

$$= 73 + 292 + 4672 \quad \text{2 additions}$$

$$= 5037$$

Mod 1000, this gives $\boxed{37}$. It took $\boxed{8}$ additions.

(b) How would you efficiently compute $2047 \cdot 7879$?

Note $2047 = 2^{11} - 1$. Thus

$$2047 \cdot 7879$$
$$= (2^{11} - 1) \cdot 7879$$
$$= 2^{11} \cdot 7879 - 7879.$$

So one method is to compute $2^{11} \cdot 7879$ through repeated doublings; this takes 11 additions.
Then, add -7879 (1 addition).
The total computation thus takes only 12 additions.

2. (a) Using the public parameters $(p, g) = (37, 2)$, Hellman sends you his public key $g^h = 5$. Your secret key is $d = 6$. Compute your shared secret with Hellman.

$$SS = (g^h)^d \pmod{37} = 5^6 \pmod{37} = \boxed{11}$$

(b) Prove that Hellman's secret $\mathrm{sk_H} = h$ is only defined mod 36, i.e., that you could imitate Hellman using any secret key of the form $\mathrm{sk_H} + 36n$, for $n \in \mathbb{Z}$.
Hint: Use Fermat's Little Theorem.

Let $n \in \mathbb{Z}$.
Then suppose we use a secret key of the form $h + 36n$.
The shared secret will then be computed as

$$(g^d)^{h+36n} \pmod{37}$$

$$= g^{dh} \cdot g^{36dn} \pmod{37}.$$

$$= g^{dh} \cdot (g^{36})^{dn} \pmod{37}.$$

By Fermat's Little Theorem, $g^{36} \equiv 1 \pmod{37}$.
Thus

$$g^{dh} \cdot (g^{36})^{dn} \pmod{37} = g^{dh} \cdot 1^{dn} \pmod{37} = g^{dh}.$$

We have thus recovered the original shared secret.

(c) Using Sun-Tzu's Remainder Theorem to compute discrete logarithms, compute Hellman's secret (mod 36).

Goal: find $h \in \mathbb{Z}$ such that $2^h \equiv 5 \pmod{37}$

Suffices to compute $h \pmod{36}$.

SRT says it suffices to compute $h \pmod 4$ and $h \pmod 9$

- We first compute $h \pmod 2$.

$$h = h_0 + 2h_1 \text{ for } h_0 \in \{0,1\}.$$

We know $2^{(p-1)/2} = 2^{18}$ has order 2.

Thus (all mod 37):

$$-1 \equiv 5^{18} \quad \text{by computation}$$
$$\equiv (2^h)^{18}$$
$$\equiv 2^{18h_0 + 36h_1}$$
$$\equiv (2^{18})^{h_0} \cdot (2^{36})^{h_1}$$
$$\equiv (-1)^{h_0}$$

since $2^{18} \equiv -1 \pmod 2$ and $2^{36} \equiv (2^{18})^2 \equiv 1 \pmod 2$

Thus $h_0 = 1$, so $h \equiv 1 \pmod 2$.

- Next we compute $h \pmod 4$. Since $h \equiv 1 \pmod 2$, there exist h_1, h_2 with $h_1 \in \{0,1\}$ such that

$h = 1 + 2h_1 + 4h_2$. (How do we know that?)

Also, we know $2^{(p-1)/4} = 2^9$ has order 4.

Thus (all mod 37):

$$6 \equiv 5^9 \quad \text{by computation}$$

$$\equiv \left(2^{1+2h_1+4h_2}\right)^9$$

$$\equiv \underbrace{2^9}_{\equiv -6} \cdot \underbrace{(2^{18})}_{\equiv -1}{}^{h_1} \cdot \underbrace{(2^{36})}_{\equiv 1 \text{ (since } 2^9 \text{ has order } 4)}{}^{h_2}$$

$$\equiv -6 \cdot (-1)^{h_1}.$$

Thus $h_1 = 1$, so $h \equiv 3 \pmod 4$.

- We next compute $h \pmod 3$. Write $h = h_0 + 3h_1$, for $h_0 \in \{0,1,2\}$. We know $2^{(p-1)/3} = 2^{12}$ has order 3. Thus (all mod 37)

$$10 \equiv 5^{12}$$

$$\equiv \left(2^{h_0+3h_1}\right)^{12}$$

$$\equiv \underbrace{(2^{12})}_{\equiv 26}{}^{h_0} \cdot \underbrace{(2^{36})}_{\equiv 1}{}^{h_1}$$

$$\equiv 26^{h_0}.$$

This means $h_0 = 2$, since $26^2 \equiv 10 \pmod{37}$.

- Now we can compute $h \pmod 9$. Since $h \equiv 2 \pmod 3$, we can write $h = 2 + 3h_1 + 9h_2$ for $h_1 \in \{0,1,2\}$. We also know $2^{(p-1)/9} = 2^4$ has order 9. Then (all mod 37):

$$33 \equiv 5^4$$
$$\equiv (2^{2+3h_1+9h_2})^4$$
$$\equiv \underset{\underset{34}{\equiv}}{2^8} + \underset{\underset{26}{\equiv}}{(2^{12})^{h_1}} + \underset{\underset{1}{\equiv}}{(2^{36})^{h_2}}$$

$$\equiv 34 \cdot 26^{h_1}.$$

Trying all 3 possible values for h_1, we find $h_1 = 1$ works.
Thus $h \equiv 5 \pmod 9$.

- We have so far shown $h \equiv 3 \pmod 4$ and $h \equiv 5 \pmod 9$. We can now use Euclid's algo to solve for $c, d \in \mathbb{Z}$ s.t. $4c + 9d = 1$: $c = -2, d = 1$ (can just do it by looking at it, in this case). Then the SRT says

$$h \equiv (5)(-2)(4) + (3)(1)(9) \pmod{36}$$
$$\equiv \boxed{23} \pmod{36}$$

And sure enough, we can verify $2^{23} \equiv 5 \pmod{37}$.

3. This questions is a toy example of RSA. You are reommended to use a computer to aid your calculations. If you are not comfortable with programming then please use Wolfram Alpha (`www.wolframalpha.com`), or better, install SageMath `www.sagemath.org` (ask if you want help using SageMath). Set $p = 307$, $q = 311$, and $n = p \cdot q$. Note that p and q are prime numbers.

   (a) Compute the RSA secret key corresponding to the RSA public key $(247, n)$.

Known: $e = 247$

$n = 307 \cdot 311 = 95{,}477$

$\varphi(n) = (p-1)(q-1) = 94{,}860$

Secret key d is given by $e^{-1} \pmod{\varphi(n)}$

$= 247^{-1} \pmod{94{,}860}$

$= \boxed{55303}$

(b) The values $m_0, m_1, m_2, m_3, m_4, m_5, m_6, m_7$ below are a message that has been encrypted using the public RSA key $(247, n)$. Decrypt this message and translate it into plaintext by assigning the value 00 to A, 01 to B, etc., up to 25 to Z, and assigning the value 26 to !.

$$m_0 = 94755$$
$$m_1 = 87565$$
$$m_2 = 41862$$
$$m_3 = 49231$$
$$m_4 = 34234$$
$$m_5 = 17479$$
$$m_6 = 26771$$
$$m_7 = 87503.$$

i	$m_i^{55303} \pmod{95477}$
0	19070
1	40013
2	18220
3	41708
4	18051
5	41719
6	24192
7	21426

Splitting this into chunks, we have:

19, 07, 04, 00, 13, 18, 22, 04, 17, 08, 18, 05, 14, 17, 19, 24, 19,

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

T H E A N S W E R I S F O R T Y T

22, 14, 26

↓ ↓ ↓

W O !

4. (a) Hellman contacts you to tell you that he wants to send you an encrypted message using ElGamal encryption. You choose parameters $p = 37$, $g = 2$, and $sk_A = 7$. Using square-and-multiply, compute your public key pk_A.

$pk_A = g^d \pmod p$

$= 2^7 \pmod{37}$

Note 7 in binary is 111.

First we <u>square</u>:

$2^{2^0} \equiv 2 \pmod{37}$

$2^{2^1} \equiv 2^2 \equiv 4 \pmod{37}$

$2^{2^2} \equiv 4^2 \equiv 16 \pmod{37}$.

Thus $2^7 \equiv 2 \cdot 4 \cdot 16 \pmod{37}$

$\equiv 128 \pmod{37}$

$\equiv \boxed{17}$

(b) Hellman replies with the ciphertext

$$(pk_H, enc_m) = (9, 13).$$

Decrypt the message. When you perform modular inversion, use Euclid's algorithm and show your working.
(Note: the 'message' is just a number mod 37).

I used public key, not secret key

$ss = pk_H^{d} \pmod p) = 9^{\cancel{17}\ 7} \pmod{37} = \cancel{32}\ 16$

Now we need to find $ss^{-1} \pmod{37}$.

$$\begin{aligned} 37 &= 32 + 5 \\ 32 &= 6(5) + 2 \\ 5 &= 2(2) + 1 \end{aligned} \implies \begin{aligned} 1 &= 5 - 2(2) \\ &= 5 - 2(32 - 6(5)) \\ &= 13(5) - 2(32) \\ &= 13(37 - 32) - 2(32) \\ &= 13(37) - 15(32) \end{aligned}$$

Thus $\cancel{32}^{\,16\ -1} \equiv -15 \equiv \cancel{22}\ 7 \pmod{37}$.

So

$$\begin{aligned} m &= enc_m \cdot ss^{-1} \pmod{37} \\ &= 13 \cdot \cancel{22}\ 7 \pmod{37} \\ &= \boxed{\cancel{27}}\ 17 \end{aligned}$$

right idea, one mistake @ beginning

(c) You ask Hellman to share the message with Bob. You observe Hellman sending the ciphertext

$$(pk_H, enc_m) = (9, 8)$$

to Bob. Compute Bob and Hellman's shared secret.

✓ (just carried an error from (b))

We know $m = enc_m \cdot SS^{-1} \pmod{p}$

$$\Longrightarrow SS = enc_m \cdot m^{-1} \pmod{p}.$$

We can compute $m^{-1} = \cancel{27}^{-1} \pmod{37} = \cancel{11}$. 24

17

from mistake in pt (b)

Thus

$$SS = 8 \cdot \cancel{11} \pmod{37}$$ 24

$$= \boxed{\cancel{14}} \quad 7$$