Homework Set 9

Problem 1

Example 15. Bob's public RSA key is $N=35$, $e=17$. Determine Bob's secret key.

Solution. The private key is $d=e^{-1} \pmod{\phi(N)}$. Here, since $\phi(35)=4\cdot 6=24$, the key is $d=17^{-1} \pmod{24}$. We compute $17^{-1} \pmod{24}$ using the extended Euclidean algorithm (or, if you are comfortable with that, using Sage):

$$\begin{aligned}\boxed{24} &= 1\cdot\boxed{17}+7\\ \boxed{17} &= 2\cdot\boxed{7}+3\\ \boxed{7} &= 2\cdot\boxed{3}+1\end{aligned}$$

Backtracking through this, we find that Bézout's identity takes the form

$$1=\boxed{7}-2\cdot\boxed{3}=\boxed{7}-2\cdot(\boxed{17}-2\cdot\boxed{7})=5\cdot\boxed{7}-2\cdot\boxed{17}=5\cdot(\boxed{24}-\boxed{17})-2\cdot\boxed{17}=5\cdot\boxed{24}-7\cdot\boxed{17}.$$

Hence, $17^{-1}\equiv -7\equiv 17 \pmod{24}$ and, so, $d=17$.

Alternatively. If you are comfortable with applying the extended Euclidean algorithm to compute inverses, you can alternatively use Sage:

```
>>> inverse_mod(17, 24)
```

17

Comment. Actually, as will be discussed in class, $\phi(N)=(p-1)(q-1)=4\cdot 6$ can be replaced with $\mathrm{lcm}(p-1,q-1)=\mathrm{lcm}(4,6)=12$. It follows that the pair $(e,d)=(17,17)$ is equivalent to the pair $(e,d)=(5,5)$.

Problem 2

Example 16. Bob's public RSA key is $N=55$, $e=31$. You intercept the encrypted message $c=7$ from Alice to Bob. Break the cipher and determine the plaintext.

Solution. First, as in the previous problem, we determine Bob's secret key: $d=e^{-1} \pmod{\phi(N)}$. Here, since $\phi(55)=4\cdot 10=40$, the key is $d=31^{-1}\equiv 31 \pmod{40}$. [It's a coincidence due to small numbers that $d=e$ again.]

Finally, we need to compute $m=c^d \pmod{N}$, that is, $m=7^{31}\equiv 18 \pmod{55}$.

Problem 3

Example 17. Bob randomly generated $N=119$ for his public RSA key. What is the smallest possible choice for e?

Solution. Recall that e must be invertible modulo $\phi(N)=\phi(7)\phi(17)=6\cdot 16$. Hence, $e=2,3,4$ are not allowed. Therefore, the smallest possible choice for e is $e=5$.

Problem 4

Example 18. Find x such that $8\equiv 3^x \pmod{19}$.

Solution. We proceed by brute-force and just go through the possibilities:

$3^2=9$, $3^3\equiv 8 \pmod{19}$

Hence, $x=3$.

As the next example shows, sometimes we might have to look for a while before finding the discrete logarithm.

[However, I have programmed the homework problem so that you will not have to search for long.]

Armin Straub
straub@southalabama.edu

Example 19. Find x such that $4 \equiv 3^x \pmod{19}$.

Solution. We proceed by brute-force and just go through the possibilities:

$3^2 = 9$, $3^3 \equiv 8$, $3^4 \equiv 8 \cdot 3 \equiv 5$, $3^5 \equiv 5 \cdot 3 \equiv -4$, $3^6 \equiv -4 \cdot 3 \equiv 7$, $3^7 \equiv 7 \cdot 3 \equiv 2$, $3^8 \equiv 2 \cdot 3 \equiv 6$, $3^9 \equiv 6 \cdot 3 \equiv -1$, $3^{10} \equiv -1 \cdot 3 \equiv -3$, $3^{11} \equiv -3 \cdot 3 \equiv -9$, $3^{12} \equiv -9 \cdot 3 \equiv -8$, $3^{13} \equiv -8 \cdot 3 \equiv -5$, $3^{14} \equiv -5 \cdot 3 \equiv 4 \pmod{19}$

Hence, $x = 14$.

Comment. As a shortcut, when we observed $3^7 \equiv 2 \pmod{19}$, we could have concluded that $4 = 2^2 \equiv 3^{7 \cdot 2} = 3^{14} \pmod{19}$ so that $x = 14$.

Problem 5

Example 20. Alice and Bob select $p = 29$ and $g = 8$ for a Diffie-Hellman key exchange. Alice sends 13 to Bob, and Bob sends 26 to Alice. What is their shared secret?

Solution. If Alice's secret is y and Bob's secret is x, then $8^y \equiv 13$ and $8^x \equiv 26 \pmod{29}$.

We compute $8^2, 8^3, \ldots \pmod{29}$ until we find either 13 or 26:

$8^2 \equiv 6$, $8^3 \equiv 6 \cdot 8 \equiv -10$, $8^4 \equiv -10 \cdot 8 \equiv 7$, $8^5 \equiv 7 \cdot 8 \equiv -2$, $8^6 \equiv -2 \cdot 8 \equiv 13 \pmod{29}$.

Hence, Alice's secret is $y = 6$. The shared secret is $(8^x)^y \equiv 26^6 \equiv 4 \pmod{29}$.

Problem 6

Example 21. Bob's public ElGamal key is $(p, g, h) = (47, 45, 14)$. Encrypt the message $m = 16$ ("randomly" select $y = 25$) for sending it to Bob.

Solution. The ciphertext is $c = (c_1, c_2)$ with $c_1 = g^y \pmod{p}$ and $c_2 = h^y m \pmod{p}$.

Here, $c_1 = 45^{25} \equiv 43 \pmod{47}$ and $c_2 = 14^{25} \cdot 16 \equiv 8 \cdot 16 \equiv 34 \pmod{47}$. Hence, the ciphertext is $c = (43, 34)$.

Problem 7

Example 22. Your public ElGamal key is $(p, g, h) = (23, 15, 8)$ and your private key is $x = 12$. Decrypt the message $c = (5, 18)$ that was sent to you.

Solution. We decrypt $m = c_2 c_1^{-x} \pmod{p}$.

Here, $m = 18 \cdot 5^{-12} \equiv 18 \cdot 5^{10} \equiv 18 \cdot 9 \equiv 1 \pmod{23}$.

Problem 8

Example 23. Bob's public ElGamal key is $(p, g, h) = (41, 29, 31)$. Determine Bob's private key.

Solution. We need to solve $29^x \equiv 31 \pmod{41}$. This yields $x = 4$.

(Since we haven't learned a better method (no "good" method is known!), you can just try $x = 1, 2, 3, \ldots$ until you find the right one.)

Problem 9

Example 24. If Bob selects $p = 23$ for ElGamal, how many possible choices does he have for g?

Solution. Since g must be a primitive root modulo p, Bob has $\phi(\phi(p)) = \phi(p - 1)$ many choices for g.

Here, Bob has $\phi(22) = 10$ choices.