MATH 158
MIDTERM 1
7 OCTOBER 2015

Name : Solutions

- The time limit is 50 minutes.
- No calculators or notes are permitted.
- For any problem asking you to write a program, you may write in a language of your choice or in pseudocode, as long as your answer is sufficiently specific to tell the runtime of the program.
- Each problem is worth 10 points.

1	/10	**2**	/10
3	/10	**4**	/10
5	/10	**6**	/10
		$\sum$	/60

(1) (a) Find integers u, v such that $91u + 74v = 1$.

	$91u+74v$	u	v
	91	1	0
	74	0	1
$91-74=$	17	1	-1
$74-4\cdot17=$	6	-4	5
$17-2\cdot6=$	5	9	-11
$6-5=$	1	-13	16

$1 = -13\cdot91 + 16\cdot74$, so $\boxed{\begin{matrix} u=-13 \\ v=16 \end{matrix}}$ is one solution.

All other solutions have the form $(-13+74k, 16-91k)$,
eg. $(61, -75)$.

(b) Find an integer x such that $74x \equiv 5 \pmod{91}$.

$74^{-1} \equiv 16 \bmod 91$, by part (a).

Hence

$$74x \equiv 5 \bmod 91$$

$$\Leftrightarrow \quad x \equiv 16\cdot5 \bmod 91$$

$$\boxed{x \equiv 80 \bmod 91}$$

(or $x \equiv -11 \bmod 91$, equivalently)

(2) Alice and Bob are performing Diffie-Hellman key exchange using the following parameters.

$$
\begin{aligned}
p &= 19 \\
g &= 2
\end{aligned}
$$

(a) Alice chooses the secret number $a = 3$. What number does she send to Bob?

$$
\begin{aligned}
A &\equiv g^a \bmod p \\
&\equiv 2^3 \bmod 19
\end{aligned}
$$

$$\boxed{A = 8}$$

(b) Bob sends Alice the number $B = 4$. What is Alice and Bob's shared secret?

$$S \equiv A^b \equiv B^a \bmod p$$

$$
\begin{aligned}
\Rightarrow \quad S &\equiv 4^3 \bmod 19 \\
&\equiv 4 \cdot 16 \bmod 19 \\
&\equiv 4 \cdot (-3) \equiv -12 \equiv 7 \bmod 19
\end{aligned}
$$

$$\boxed{S = 7}$$

(3) Alice and Bob are using the ElGamal cryptosystem, with the following parameters.

$$p = 13$$
$$g = 7$$

(a) Alice chooses the private key $a = 2$. What is her public key, A?

$$A \equiv g^a \bmod p$$
$$\equiv 7^2 \bmod 13$$
$$\equiv 49 \equiv 10 \bmod 13$$
$$\boxed{A = 10}$$

(b) Suppose that Alice receives the ciphertext $(c_1, c_2) = (2, 6)$ from Bob. What is the corresponding plaintext?

$$C_2 \equiv C_1^a \cdot m \bmod p$$
$$\Rightarrow \quad 6 \equiv 2^2 m \bmod 13$$
$$\Rightarrow \quad 4m \equiv 6 \bmod 13$$

now, $4 \cdot 10 = 40 \equiv 1 \bmod 13$, so $4^{-1} \equiv 10 \bmod 13$, and

$$m \equiv 4^{-1} \cdot 6 \bmod 13$$
$$\equiv 10 \cdot 6 \equiv 60 \equiv 8 \bmod 13$$

$$\boxed{m = 8}$$

(4) Suppose that p is a prime number at most n bits in length, and a is an element of $(\mathbf{Z}/p)^{\times}$. Write a function `inverse(a,p)` which takes the integers a, p as arguments and returns the inverse of a modulo p. For full points, your function should perform at most $\mathcal{O}(n)$ arithmetic operations, and the return value should be an integer between 1 and $p-1$ inclusive.

Solution using the extended Euclidean algorithm: (works whether p is prime or not)

```
def inverse(a,p):
    s0, u0  =  p, 0      # each s,u is part of an equation s=au+pv
    s1, u1  =  a, 1      #we will shrink s to one in stages.
    while s1 ≠ 0:
        k = s0/s1
        s2,u2 = s0-k*s1, u0-k*u1   # perform a row operation
        s0, u0 = s1, u1
        s1, u1 = s2, u2            #replace the older s,u with the newest
    return u0 %p
```

Alternative solution: compute a^{p-2} mod p. By Fermat's little theorem, this will be a^{-1} mod p.

This is $O(n)$ as long as a fast powering algorithm is used.

(5) (a) Let p be a prime, and $a \in (\mathbf{Z}/p)^\times$. Define the *order of a modulo p*.

$\mathrm{ord}_p(a) =$ the minimum positive integer e such that $a^e \equiv 1 \bmod p$.

(b) Let $p = 2^{16} + 1$ (this number is known to be prime). Prove that for any $a \in (\mathbf{Z}/p)^\times$ except 1, $\mathrm{ord}_p(a)$ is even. You may use any facts proved in the class or on the homework.

We proved on the homework that

$$\mathrm{ord}_p(a) \mid (p-1),$$

hence $\mathrm{ord}_p(a) \mid 2^{16}$, so $\mathrm{ord}_p(a)$ is a power of 2. Unless it is 1, it must be even; the only order-1 element is $1 \bmod p$.

Hence if $a \not\equiv 1 \bmod p$, then $\mathrm{ord}_p(a)$ is even.

(problem continues on next page)

(c) Suppose that $p = 2^{16} + 1$, as in the previous part. What is $\text{ord}_p(2)$?

$\text{ord}_p(2) \mid 2^{16}$, so it must be one of $1, 2, 4, \cdots, 2^{15}, 2^{16}$.

Note that $2^{16} \equiv -1 \mod p$, (so $\text{ord}_p(2) \nmid 16$)

but $2^{32} \equiv (2^{16})^2 \equiv (-1)^2 \equiv 1 \mod p$. so $\text{ord}_p(2) \mid 32$.

The only possibility is that $\boxed{\text{ord}_p(2) = 32}$

(d) Suppose that p is a prime with the property that $\text{ord}_p(a)$ is even for every $a \in (\mathbf{Z}/p)^\times$ except 1. Prove that $p = 2^n + 1$ for some integer n. You may use any facts proved in the class or on the homework.

Let q be any prime factor of $p-1$. Then if g is a primitive root, $g^{\frac{p-1}{q}}$ has order q modulo p. Since all order (besides 1) must be even, q must be even, so $q = 2$.

Therefore 2 is the only prime factor of $p-1$. It follows that, factoring $p-1$ into primes,

$$p - 1 = 2^n \quad \text{for some } n.$$

This gives the desired result.

(6) Alice and Bob have chosen parameters p, g (p is a prime, $g \in (\mathbf{Z}/p)^{\times}$) for Diffie-Hellman key exchange.

On Monday, Alice sends Bob the number A, Bob sends Alice the number B, and they establish a shared secret S.

On Tuesday, Alice sends Bob the number A', Bob sends Alice the number B', and they establish a shared secret S'.

Eve intercepts A, B, A', and B' (as usual), and she also manages to steal the first shared secret S from a post-it note in Bob's trash Monday night. Suppose that she also discovers the following two facts (possibly resulting from lazy random number generation by Alice and Bob).

$$\begin{aligned} A' &\equiv g^2 A \pmod{p} \\ B' &\equiv B^2 \pmod{p} \end{aligned}$$

How can Eve can use this information to efficiently compute the second shared secret S'?

Observe that if a, b, a', b' are the corresponding secret keys.

$$A' \equiv g^{a'} \equiv g^{a+2}$$

& $$B' \equiv g^{b'} \equiv g^{2b}.$$

Therefore

$$\begin{aligned} S \equiv g^{a'b'} &\equiv (g^{a'})^{b'} \equiv (g^{a+2})^{b'} \mod p \\ &\equiv (g^{b'})^{a+2} \equiv (g^{2b})^{a+2} \mod p \\ &\equiv g^{2ab+4b} \mod p \\ &\equiv (g^{ab})^2 \cdot (g^{b})^4 \mod p \\ &\equiv S^2 \cdot B^4 \mod p. \end{aligned}$$

So Eve can find the second secret S' by computing $S^2 \cdot B^4$ and reducing modulo p.

(additional space for work)