# Cryptography Midterm Solutions

1. Here the Euclidean algorithm has been used to show that $\gcd(96, 25) = 1$.

| *Step* | $a$ | $=$ | $b$ | $\cdot$ | $q$ | $+$ | $r$ |
|---|---|---|---|---|---|---|---|
| 1 | 96 | $=$ | 25 | $\cdot$ | 3 | $+$ | 21 |
| 2 | 25 | $=$ | 21 | $\cdot$ | 1 | $+$ | 4 |
| 3 | 21 | $=$ | 4 | $\cdot$ | 5 | $+$ | 1 |
| 4 | 4 | $=$ | 1 | $\cdot$ | 4 | $+$ | 0 |

   (a) Use the extended Euclidean algorithm to write 1 as a linear combination of 96 and 25.

   (b) What is the (multiplicative) inverse of 25 modulo 96?

   **Sol:** Working backwards.

$$\begin{aligned} 1 &= 21 - 4 \cdot 5 \\ &= 21 - (25 - 21) \cdot 5 \\ &= 25 \cdot -5 + 21 \cdot 6 \\ &= 25 \cdot -5 + (96 - 25 \cdot 3) \cdot 6 \\ &= 96 \cdot 6 + 25 \cdot -23 \end{aligned}$$

   Thus $1 = 6(96) - 23(25)$. This implies that $-23(25) \equiv 1 \mod 96$ and so $73 = -23$ is the inverse of 25 modulo 96.

2. Solve the congruence $x^{25} \equiv 12 \mod 97$.

   **Sol:** As 97 is prime, $x^{96k+1} = x$ for all integers $k$. Inparticular $12^{25^{-1}} = x^{25 \cdot 25^{-1}} = x$ where $25^{-1}$ is the multiplicative inverse of 25 modulo 96. We computed this as 73 in the last question. So the solution is $12^{73} \mod 97$. (Fast powering gives that this is $12^{64} \cdot 12^8 \cdot 12$, which would take 6 multiplications modulo 97 to evaluate. This takes too long.)

3. Find an integer $x$ satisfying the congruences $x \equiv 5 \mod 31$ and $x \equiv 12 \mod 33$.

   **Sol:** From the first congruence $x = k \cdot 31 + 5$ for some $k$. From the second $k \cdot 31 + 5 \equiv 12 \mod 33$ implying that $k \cdot 31 \equiv 7 \mod 33$. It is easy to see that the inverse of $31 = -2$ modulo 33 is $-17 = 16$ (or you could use the Euclidean Algorithm) so multiplying both sides of the previous congruence we get $k \equiv 7 \cdot 16 = 16 + 3(-1) = 13 \mod 33$. Thus $x = 5 + 13 \cdot 31$ is a solution to the congruence.

4. (a) Determine whether or not 5 is a generator (primitive root) modulo 23.

   **Sol:** The divisors of 22 are $1, 2, 11$, and 23. So by Fermat's Little Theorem we have to check if either of $5^2$ and $5^{11}$ are 1 mod 23.

- $5^2 = 25 \equiv 2 \mod 23$
- $5^{11} = 5^{2(5)+1} \equiv 2^5 \cdot 5 = 32 \cdot 5 \equiv 9 \cdot 5 = 45 \equiv -1 \mod 23$.

So yes, 5 is a generator.

(b) Evaluate $\log_2(9)$ modulo 23 ( where 2 is a generator modulo 23).

**Sol:** Just compute the powers of 2 until yoy get 5: $2^5 = 32 \equiv 9 \mod 23$ )

5. For integers $a$ and $b$ with $g = \gcd(a, b)$ let $u$ and $v$ be integers such that $ua + vb = g$. Show that if $u_0$ and $v_0$ are another pair of integers satisfying $u_0a + v_0b = g$ then for some integer $k$, $u = u_0 + kb/g$ and $v = v_0 - ka/g$.

**Sol:** Indeed, $ua + vb = g = u_0a + v_0b$ implies that $(u - u_0)a = b(v_0 - v)$. Letting $a = a'g$ and $b = b'g$ where $a'$ and $b'$ are relatively prime, this reduces to $(u - u_0)a' = b'(v_0 - v)$ from which we get that $a'|b'(v_0 - v)$ and so $a'|(v_0 - v)$. So letting $k = (v_0 - v)/a'$ and solving for $u$ we get

$$u = u_0 + b'k = u_0 + (b/g)k.$$

Now plugging $(u - u_0) = (b/g)k$ into $(u - u_0)a = b(v_0 - v)$ and solving for $v$ gives $v = v_0 - ka/g$.

6. Let $p$ be prime and $q$ be an integer dividing $p - 1$. Show that

$$\left|\{a \in (\mathbb{Z}/p\mathbb{Z})^* \mid a^{(p-1)/q} = 1\}\right| = (p - 1)/q.$$

**Sol:** As $p$ is prime, there is a generator $g$ of $(\mathbb{Z}/p\mathbb{Z})^*$, so $(\mathbb{Z}/p\mathbb{Z})^* = \{g^1, \ldots, g^{p-1}\}$. For an element $g^d$, we have $(g^d)^{(p-1)/q} = g^{d(p-1)/q} = 1$ if and only if $(p - 1)|d(p - 1)/q$. This is true if and only if $q|d$. There are $p - 1/q$ multiples of $q$ between $q$ and $p - 1$, so $(g^d)^{(p-1)/q} = 1$ for $p - 1/q$ values of $d$.

7. Recall that in the El-Gamal PKC for a prime $p$ and generator $g$, there is a public key $A(= g^a)$ where $a$ is secret. A message $m$ is encrypted to $c_1 = g^k$ and $c_2 = mA^k$ for some secret $k$. (Everything is in $(\mathbb{Z}/p\mathbb{Z})^*$).

(a) Knowing the secret key $a$ how would you decrypt $(c_1, c_2)$ to $m$? (You of course know $p, g$, and $A$ as well.)

**Sol:** Inverting $c_2^a$ modulo $p$ we calculate:

$$c_1(c_2^{-a}) = mA^k g^{-ak} = mg^{ak}g^{-ak} = m.$$

(b) What is the Diffie-Hellman Problem for a prime $p$ and generator $g$ modulo $p$.

**Sol:** Knowing $g$ and $p$, we are given $A = g^a$ and $B = g^b$ in $(\mathbb{Z}/p\mathbb{Z})^*$, and must find $g^{ab}$.

(c) Assuming that you have an oracle for the Diffie-Hellman problem, explain how you could crack the El-Gamal PKC: that is, quickly find $m$ without using $a$.

**Sol:** Taking $A = A = g^a$ and $B = c_1 = g^k$, the oracle for the Diffie-Hellman problem gives us $g^{ak}$. Inverting this we get $g^{-ak}$ and then multiplying by $c_2$ we get

$$c_2 g^{-ak} = mA^k g^{-ak} = mg^{ak} g^{-ak} = m,$$

as needed.

8. Suppose that $\gcd(a, pq) = 1$ for distinct odd primes $p$ and $q$. Prove that if the equation $x^2 \equiv a \mod pq$ has any solutions, then it has 4 solutions.

**Sol:** Assume that there is a solution $x_0 \bmod pq$. Then $x_p = x_0 \bmod p$ is a solution mod $p$ (ie. to $x^2 \equiv a \mod p$). Because $\gcd(a, p) | \gcd(a, pq) = 1$, $a$ and so $x_p$, is non-zero modulo $p$. As $p$ is not even, $-x_p$ is another solution (distinct from $x_p$) modulo $p$. Similarily there are two distinct solutions $x_q$ and $-x_q \bmod q$. Each choice of a solution $z_p \bmod p$ and a solution $z_q \bmod q$ lifts by the CRT to a solution $z \bmod pq$. (As the image $z$ modulo $p$ is $z_p$ and modulo $q$ is $z_q$, each choice of $z_q$ and $z_p$ lifts to a distinct solution $z$.) So there are four such solutions.

| Question | Out of | Score |
|---|---|---|
| 1 | 3 | |
| 2 | 3 | |
| 3 | 3 | |
| 4 | 3 | |
| 5 | 3 | |
| 6 | 3 | |
| 7 | 3 | |
| 8 | 3 | |
| Total | 24 | |