C&O 685
The Mathematics of Public-Key Cryptography

Midterm (with solutions)

November 2, 2000

Questions

1. (7 marks)

   (a) Factor 100 into prime powers.
   Solution: $100 = 2^2 5^2$.

   (b) Briefly describe how you would *efficiently* verify that a given element $\alpha \in \mathbb{Z}_{101}{}^*$ is a primitive element.
   Solution: $\alpha \in \mathbb{Z}_{101}{}^*$ is a primitive element if and only if $\alpha^{100/p} \not\equiv 1 \pmod{101}$ for $p \in \{2, 5\}$.

   (c) Use the technique described above to determine if 60 is a primitive element modulo 101. Here are some pre-computed powers of 60 modulo 101 to make the computations easier:

   $$\begin{aligned} &60^2 \bmod 101 = 65, \\ &60^4 \bmod 101 = 84, \\ &60^8 \bmod 101 = 87, \\ &60^{16} \bmod 101 = 95, \text{ and} \\ &60^{32} \bmod 101 = 36. \end{aligned}$$

   Solution: $60^{20} \equiv 60^{16} 60^4 \equiv 95 \times 84 \equiv 1 \pmod{101}$, so 60 is not primitive.

2. (7 marks) Suppose that p and q are distinct odd primes, and $y \in \mathbb{Z}_{pq}{}^*$.

   (a) Briefly describe how you would determine quickly if y has square roots in $\mathbb{Z}_{pq}{}^*$.
   Solution: y has square roots in $\mathbb{Z}_{pq}{}^*$ if and only if the Legendre symbols $(\frac{y}{p}) = (\frac{y}{q}) = 1$.

   (b) Assuming that $p \equiv 3 \bmod 4$ and $q \equiv 3 \bmod 4$, briefly describe how you would compute the square roots of y in $\mathbb{Z}_{pq}{}^*$.
   Solution: First check that $(\frac{y}{p}) = (\frac{y}{p}) = 1$. Then compute $x_p = y^{(p+1)/4} \bmod p$ and $x_q = y^{(q+1)/4} \bmod q$. Finally, use the Chinese remainder theorem to find $x \in \mathbb{Z}_{pq}{}^*$ such that $x \equiv \pm x_p \pmod{p}$ and $x \equiv \pm x_q \pmod{q}$.

   (c) Given the ciphertext $y = 16$, obtained from the Rabin system in $\mathbb{Z}_{77}{}^*$, compute the four possible plaintexts that encrypt to y (i.e., find the four square roots of y modulo 77).
   Solution: Let $p = 7$ and $q = 11$. Then $x_p = 16^2 \bmod 7 = 2^2 \bmod 7 = 4$ and $x_q = 16^3 \bmod 11 = 5^3 \bmod 11 = 125 \bmod 11 = 4$. The solution to the system $x \equiv \pm 4 \bmod 7$, $x \equiv \pm 4 \bmod 11$ is $x \equiv \pm 4, \pm 18 \pmod{77}$.

3. (7 marks) Suppose p is an odd prime. State and prove Euler's Criterion for determining if an element $x \in \mathbb{Z}_p{}^*$ is a quadratic residue modulo p. (You can assume that the multiplicative group $\mathbb{Z}_p{}^*$ is cyclic.)
Solution: See the proof of Theorem 4.8 in the textbook.

4. (7 marks) Suppose that $n = 4633$.

   (a) For $x = 68, 69$ and 96, compute $x^2 \bmod n$.
   Solution: $68^2 \bmod n = 4630$, $69^2 \bmod n = 128$ and $96^2 \bmod n = 4583$.

(b) Factor these three integers $x^2 \bmod n$ over the factor base $\{-1, 2, 3, 5\}$.
Solution: $68^2 \bmod n = (-1) \times 3$, $69^2 \bmod n = 2^7$ and $96^2 \bmod n = (-1) \times 2 \times 5^2$.

(c) Using these three factorizations, construct a congruence of the form $y^2 \equiv z^2 \bmod n$ and find a non-trivial factor of n by computing a gcd.
Solution: $(68 \times 69 \times 96)^2 \equiv (2^4 \times 3 \times 5)^2 \pmod{n}$. This simplifies to yield $1031^2 \equiv 240^2 \pmod{n}$. Now compute $\gcd(1031 - 240, n) = 41$ to obtain a factor of n.

5. (7 marks) Use the Pollard Rho algorithm to compute the logarithm of of $\beta = 41$ to the base $\alpha = 4$, in the subgroup $\langle\alpha\rangle$ of $\mathbb{Z}_{83}{}^*$. Note that $\alpha = 4$ has order $n = 41$. Begin with the initial triple $(1, 0, 0)$, so $x_0 = 1$. Find the smallest positive integer i such that $x_i = x_{2i}$, and proceed to compute the desired discrete logarithm. The partition of $\mathbb{Z}_{83}{}^*$ into $S_1 \cup S_2 \cup S_3$ is defined as follows:

$$\begin{aligned} &x \in S_1 \text{ if } x \equiv 1 \bmod 3;\\ &x \in S_2 \text{ if } x \equiv 0 \bmod 3; \text{ and}\\ &x \in S_3 \text{ if } x \equiv 2 \bmod 3. \end{aligned}$$

The x-values are updated as follows:

$$\begin{aligned} &\text{if } x \in S_1, \text{ then } x \leftarrow x\beta;\\ &\text{if } x \in S_2, \text{ then } x \leftarrow x^2; \text{ and}\\ &\text{if } x \in S_3, \text{ then } x \leftarrow x\alpha. \end{aligned}$$

Hint: The value i mentioned above is very small.
Solution: We compute the following:

i	(x_a, a_i, b_i)
0	$(1, 0, 0)$
1	$(41, 0, 1)$
2	$(81, 1, 1)$
3	$(4, 2, 2)$
4	$(81, 2, 3)$

Since $x_2 = x_4$, we compute $\log_4 41 = (1 - 2)(3 - 1)^{-1} \bmod 41 = (-1) \times 21 \bmod 41 = 20$.

6. (12 marks) A common way to speed up RSA decryption incorporates the Chinese remainder theorem, as follows. Suppose that $d_K(y) = y^a \bmod n$ and $n = pq$, where p and q are distinct odd primes. Define $a_p = a \bmod (p - 1)$ and $a_q = a \bmod (q - 1)$; and let $M_p = q^{-1} \bmod p$ and $M_q = p^{-1} \bmod q$. Then consider the following algorithm:

input:	n, a_p, a_q, M_p, M_q, y
1.	$x_p \leftarrow y^{a_p} \bmod p$
2.	$x_q \leftarrow y^{a_q} \bmod q$
3.	$x \leftarrow M_p q x_p + M_q p x_q \bmod n$
output:	x

(a) Prove that the value x returned by the above algorithm is, in fact, $y^a \bmod n$ (the proof is quite short!).
Solution: $a \equiv a_p \pmod{p-1}$ implies $y^a \equiv y^{a_p} \pmod{p}$, so $y^a \equiv x_p \pmod{p}$. Similarly, $a \equiv a_q \pmod{q-1}$ implies $y^a \equiv y^{a_q} \pmod{q}$, so $y^a \equiv x_q \pmod{q}$. However, it is also the case that $x \equiv x_p \pmod{p}$ and $x \equiv x_q \pmod{q}$. Therefore, applying the Chinese remainder theorem, it follows that $x \equiv y^a \pmod{n}$.

(b) Given that $p = 11$, $q = 13$ and $a = 83$, compute a_p, a_q, M_p and M_q. (Note: you can make use of the equation $6 \times 11 - 5 \times 13 = 1$.)
Solution: $a_p = 3$, $a_q = 11$, $M_p = 6$ and $M_q = 6$.

(c) Given the above values of p, q, and a, decrypt the RSA ciphertext $y = 54$ using the above algorithm.
Solution: $x_p = 54^3 \bmod 11 = 10^3 \bmod 11 = 10$ and $x_q = 54^{11} \bmod 13 = 2^{11} \bmod 13 = 7$. Then $x = 6 \times 13 \times 10 + 6 \times 11 \times 7 \bmod n = 98$.