MATH UN3025 - Midterm 1 Solutions

1. (10 pts.) Suppose you have a language with only 3 letters: A, B, and C, which occur with frequencies $0.7, 0.2$, and 0.1, respectively. The following ciphertext was encrypted by the Vigenère method:

$$BABABCBCAC.$$

Assume that the key length is either 1, 2, or 3. Find the most likely key length and determine the most likely key using the method from class.

Solution: We compare $BABABCBCAC$ with its shifts by 1, 2, and 3, looking for overlaps. There are no overlaps for a shift of 1 or 3, but there are 6 overlaps for a shift of 2. Thus we expect the key length to be 2.

Looking at every other letter, we see $BBBBA$ and $AACCC$ for the letters in even and odd positions, respectively. Due to the overwhelming frequency of the letter A in the language, we can reasonably assume that B decrypts to to A in the first sequence and C decrypts to A in the second. This gives us the key BC.

2. Solve the following problems about modular arithmetic.

(a) (5 pts.) Use the Euclidean algorithm to find the greatest common divisor d of the numbers 123 and 270.

Solution: The Euclidean algorithm gives

$$\begin{aligned} 270 &= 2 \cdot 123 + 24 \\ 123 &= 5 \cdot 24 + 3 \\ 24 &= 6 \cdot 3. \end{aligned}$$

This means that $d = 3$, the last nonzero remainder.

(b) (5 pts.) Use the extended Euclidean algorithm to write the number d from part (a) as

$$d = a \cdot 123 + b \cdot 270$$

for some integers a, b.

Solution: Use the extended Euclidean algorithm.

$$x_0 = 0, x_1 = 1, x_2 = -2 \cdot 1 + 0 = -2, x_3 = -5 \cdot (-2) + 1 = 11.$$

$$y_0 = 1, y_1 = 0, y_2 = -2 \cdot 0 + 1 = 1, y_3 = -5 \cdot 1 + 0 = -5.$$

So $11 \cdot 123 - 5 \cdot 270 = 3$.

(c) (5 pts.) Find all solutions $x \pmod{270}$ to the linear equation

$$123x \equiv 6 \pmod{270}.$$

Solution: Divide by 3 to get $41x_0 \equiv 2 \pmod{90}$. We divide $11 \cdot 123 - 5 \cdot 270 = 3$ by 3 to get $11 \cdot 41 - 5 \cdot 90 = 1$, so $41^{-1} \equiv 11 \pmod{90}$. Thus $x_0 \equiv 2 \cdot 11 \equiv 22 \pmod{90}$, and the solutions are $22, 22 + 90 = 112$, and $22 + 180 = 202 \pmod{270}$.

3. (5 pts.) What are the last two digits of the number 4321^{642}?

Solution: Reduce 4321 modulo 11 and 642 modulo $\phi(100) = 40$ to get $21^2 \equiv 41 \pmod{100}$.

4. (10 pts.) Use the Chinese Remainder Theorem to find a number x modulo $5 \cdot 7 \cdot 8 = 280$ such that

$$x \equiv 1 \pmod{5}, x \equiv 2 \pmod{7}, x \equiv 3 \pmod{8}.$$

Solution: Use the method from class, with $m_1 = 5, m_2 = 7, m_3 = 8$, $a_1 = 1$, $a_2 = 2$, and $a_3 = 3$. We have

$$z_1 = m_2 \cdot m_3 = 56, z_2 = m_1 \cdot m_3 = 40, z_3 = m_1 \cdot m_2 = 35,$$

$$y_1 = 56^{-1} \equiv 1 \pmod 5, y_2 \equiv 40^{-1} \equiv 3 \pmod 7, y_3 \equiv 35^{-1} \equiv 3 \pmod 8.$$

Then we calculate

$$x = 1 \cdot 56 \cdot 1 + 3 \cdot 40 \cdot 2 + 3 \cdot 35 \cdot 3 = 56 + 240 + 315 = 611 \equiv 51 \pmod{280}.$$

5. Answer the following questions about the ElGamal cryptosystem.
(a) (2 pts.) State the ElGamal public key cryptosystem.
Solution: Bob's public key is (p, α, β) where α is primitive mod p and $\beta \equiv \alpha^a \pmod p$ for some private integer a.
To encrypt m, Alice picks a random integer k, computes $r \equiv \alpha^k \pmod p$ and $t \equiv m\beta^k \pmod p$, and sends (r, t) to Bob.
Bob decrypts by calculating $m \equiv r^{-a} \cdot t \pmod p$.
(b) (2 pts.) State the Computational Diffie Hellman Problem (CDHP).
Solution: Fix (p, α), where α is primitive mod p. Given α^x and $\alpha^y \pmod p$, the CDHP is to compute $\alpha^{xy} \pmod p$.
(c) (6 pts.) Explain why breaking the ElGamal cryptosystem is equally hard as solving the CDHP.
Solution: Given a box that breaks ElGamal, plug in $\beta = \alpha^x$, $r = \alpha^y$, $t = 1$, so $a = x$. Then the output will give $r^{-a} \cdot t \equiv \alpha^{-xy} \pmod p$. One can now compute the inverse to get $\alpha^{xy} \pmod p$.
Given a box that breaks the CDHP, plug in $\alpha^a \equiv \beta \pmod p$ and $\alpha^k \equiv r \pmod p$ to get $\alpha^{ak} \pmod p$ out. Then compute the message as $(\alpha^{ak})^{-1} \cdot t \pmod p$.
6. (10 pts.) Use the Pohlig-Hellman algorithm from class to find the discrete log $L_2(11)$ for the prime $p = 13$. You may assume that 2 is a primitive root modulo 13.
Solution: $13 - 1 = 2^2 \cdot 3$. Let $\beta = 11$.
First consider $q^a = 2^2$. Write $x \equiv x_0 + x_1 \cdot 2 \pmod 4$. Since 2 is primitive, $2^{\frac{13-1}{2}} \equiv 2^6 \equiv -1 \pmod{13}$. We have $\beta^{\frac{p-1}{q}} \equiv 11^{\frac{13-1}{2}} \equiv (-2)^6 \equiv -1 \pmod{13}$, so $x_0 = 1$. We define $\beta_1 \equiv \beta \cdot \alpha^{-x_0} \equiv 11 \cdot 2^{-1} \equiv 11 \cdot 7 \equiv -1 \pmod{13}$. Then $\beta_1^{\frac{p-1}{q^2}} \equiv (-1)^3 \equiv -1 \pmod{13}$, so $x_1 = 1$ as well. This gives $x \equiv 3 \pmod 4$.
Now consider $q^a = 3^1$. Write $x \equiv x_0 \pmod 3$. We have $\alpha^{\frac{p-1}{3} x_0} \equiv 2^{4x_0} \equiv 3^{x_0} \pmod{13}$. For $x_0 = 0, 1, 2$, we respectively have $3^{x_0} \equiv 1, 3, 9 \pmod{13}$. We have $\beta^{\frac{p-1}{3}} \equiv (-2)^4 \equiv 3 \pmod{13}$, so we must have $x_0 = 1$, or $x \equiv 1 \pmod 3$.
We use the CRT to deduce from $x \equiv 3 \pmod 4$ and $x \equiv 1 \pmod 3$ that $x \equiv 7 \pmod{12}$.
Extra credit. Suppose that Alice has encrypted and sent a message m to Bob using RSA, where the public key is (n, e). Assume that n is very large, but m is short, approximately around 10^{17}.
(a) (4 pts.) If Eve has intercepted the ciphertext c, explain how she can use the short plaintext attack from class to try to find m.
Solution: For each $0 \le x < 10^9$ and $0 \le y < 10^9$ calculate cx^{-e} and $y^e \pmod n$. Check efficiently whether there is a match between the two lists, e.g. by sorting the first list and doing binary search for each member of the second. If $cx^{-e} \equiv y^e \pmod n$, then $c \equiv (xy)^e \pmod n$, which implies $m \equiv xy \pmod n$ or $m = xy$.
(b) (1 pt.) Explain why this attack is faster than encrypting all possible m's of size around 10^{17}.
Solution: The attack requires on the order of 2×10^9 computations (multiplied by a log factor coming from sorting/binary search), which is far smaller than the 10^{17} calculations required to encrypt all possible m's.
(c) (1 pt.) Explain the conditions on m for this attack to be successful.
Solution: The number m must be a product of two numbers, x and y, in the range $0 \le x, y < 10^9$. Not all m's have this property – for instance, if m has a prime divisor larger than 10^9, this is impossible. Conversely, if m is equal to such a product, the algorithm will find m.