

4261 Midterm Solutions

1. Short Answer. Unjustified numerical answers receive no credit.

(a) (8 points) What are the last 2 digits of 2004^{2004} base-10? **Solution:** 64. To see this notice that we are asking what the value of 2004^{2004} modulo 100. Exponentiating mod-100 is the same as evaluating the exponent mod- $\phi(100)$ by Lagrange's theorem. $\phi(100) = \phi(25) \cdot \phi(4) = 20 \cdot 2 = 40$. Thus $2004^{2004} \bmod 100 = 4^4 \bmod 100 = 56$.

(b) (8 points) What is the probability that a random element in \mathbb{Z}_{16001}^* is primitive? You may assume that 16,001 is prime. **Solution:** The following formula for this probability was given in lecture: $\frac{\phi(p-1)}{p-1}$. For $p = 16,001$, we have $p - 1 = 16,000 = 2^7 \cdot 5^3$ so $\phi(p - 1) = 2^6 \cdot 4 \cdot 5^2 = 2^8 \cdot 5^2$ and the probability of getting a primitive element is $\frac{2^8 \cdot 5^2}{2^7 \cdot 5^3} = 0.4$.

(c) (8 points) How many cube roots does 7 have in \mathbb{Z}_{33}^* ?

Solution: Exactly one: since $\phi(33) = 20$ which is relatively prime to 7, the function $f(x) = x^3 \bmod 33$ is invertible with inverse $g(x) = x^{3^{-1} \bmod 20} \bmod 33$ so that the unique cube root of 7 is just $g(7)$.

(d) (8 points) How many square roots does 9 have in \mathbb{Z}_{561} ?

Solution: Four: Factor $561 = 3 \cdot 11 \cdot 17$. Find the square roots of 9 in each of the moduli. mod-3, 9 is 0 so only has one square root: 0. mod-11, 9 has the square roots ± 3 . mod-17, 9 has the square roots ± 3 . The CRT implies that square roots of 9 mod 561 arise from all possible combination of square roots of 9 mod each moduli. So the total number of square roots is the product of the number in each modulus, namely $1 \cdot 2 \cdot 2 = 4$.

(e) (8 points) It is known that 5 and 13 are primitive in \mathbb{Z}_{47}^* . The following equation has been discovered: $5^9 13^{21} \equiv_{47} 5^{13} 13^{29}$. Find $\text{Dlog}_{13}(5) \bmod 47$.

Solution: $\text{Dlog}_{13}(5) \bmod 47 = 21$.

2. (40 points) Block Ciphers and Perfect Secrecy.

Described below are two block ciphers BC_a, BC_b . In each case, plaintexts and ciphertexts are 64-bit blocks so $\mathcal{P} = \mathcal{C} = \mathbb{Z}_2^{64}$. Keyspace \mathcal{K} and encryption and decryption functions are defined below. One of the block ciphers satisfies perfect secrecy, while the other does not. Determine whether the given block cipher is perfect¹. Prove your claim in each case.

(a) For BC_a we view each block as describing a 64-bit number so cipherspace/plainspace is identified with $\mathbb{Z}_{2^{64}}$. Keys are 64 bits long as well, but we view the first 63 bits as describing a number in $\mathbb{Z}_{2^{63}}$ and the last bit as a number in \mathbb{Z}_2 ; in other words,

¹Here we are only asking if the block cipher is perfect when a single block is transmitted; neither will be perfect if more than one block is transmitted per key.

$\mathcal{K} = \mathbb{Z}_{2^{63}} \times \mathbb{Z}_2$. For a key $K = (m, n)$ with $m \in \mathbb{Z}_{2^{63}}, n \in \mathbb{Z}_2$ view m, n as residing in $\mathbb{Z}_{2^{64}}$ and define encryption by setting $e_{(m,n)}(x) = (2m + 1)x - n$.

Solution: NOT PERFECTLY SECURE. Not every ciphertext is achievable from every plaintext. For example, consider $x = 0^{64}$. Numerically, this is just zero. Consequently, $e_{(m,n)}(x) = e_{(m,n)}(0) = (2m + 1) \cdot 0 - n = -n$. Thus $\Pr[e_K(0^{64}) = 0^{64}] = \Pr[n = 0] = 0.5$. On the other hand, if we start with the plaintext $x' = 0^{63}1$ -representing the numerical value 1- every ciphertext is achievable with equal probability since $e_{(m,n)}(x') = e_{(m,n)}(1) = (2m + 1) \cdot 1 - n = 2m + (1 - n)$ so that all the odd numbers in $\mathbb{Z}_{2^{64}}$ are enumerated for $n = 0$ while all even numbers for $n = 1$. In particular, the probability of any particular ciphertext is 2^{-64} . I.e. $\Pr[e_K(0^{63}1) = 0^{64}] = 2^{-64}$. But this violates the requirements of message indistinguishability because letting $x = 0^{64}, x' = 0^{63}1$ and $y = 0^{64}$ we have $\Pr[e_K(x) = y] \neq \Pr[e_K(x') = y]$ thus disproving perfect security.

- (b) BC_b is defined as follows: $\mathcal{K} = \mathbb{Z}_2^{128}$. Encryption is given by $e_k(x) = \sigma(x) \oplus k_L \oplus k_R^R$. Here σ is some fixed 64-bit (one-to-one) substitution, k_L is the left half of k (the first 64 bits) and k_R^R is the reversal of the right half of k .

Solution: PERFECTLY SECURE. Compute the probability that given plaintexts go to given ciphertexts. $\Pr[e_k(x) = y] = \Pr[\sigma(x) \oplus k_L \oplus k_R = y] = \Pr[k_L \oplus k_R = y \oplus x]$. For a fixed value of k_L , there is exactly one value of k_R , namely $y \oplus x \oplus k_L$ which satisfies the last condition. So we have the following conditional probability: $\Pr[k_L \oplus k_R = y \oplus x \mid k_L] = 2^{-64}$. Using the sum-rule for probabilities we have: $\Pr[k_L \oplus k_R = y \oplus x] = \sum_{k_L} \Pr[k_L \oplus k_R = y \oplus x \mid k_L] \cdot \Pr[k_L] = \sum_{k_L} 2^{-64} \cdot 2^{-64} = 2^{64} \cdot 2^{-128} = 2^{-64}$. I.e., given any ciphertext, all plaintexts map to it with equal probability showing that the cryptosystem is message indistinguishable so perfectly secure.

3. Classical Cryptography. Consider the following generalization of the Hill cipher where instead of only multiplying by a matrix, we also add a vector. In particular, $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^n$ (n -dimensional column vectors), $\mathcal{K} = M_n(26)^* \times \mathbb{Z}_{26}^n$ where each key K is composed by an invertible matrix and vector, i.e. $K = (M, v)$ and encryption is defined by $e_K(x) = Mx + v$.

- (a) (8 points) Suppose we know that the ciphertext is $y = \begin{pmatrix} 24 \\ 15 \end{pmatrix}$, and that the key was

$$K = \left(\begin{pmatrix} 11 & 4 \\ 1 & 17 \end{pmatrix}, \begin{pmatrix} 5 \\ 9 \end{pmatrix} \right). \text{ What is the plaintext } x? \text{ Justify.}$$

Solution: $x = \begin{pmatrix} 13 \\ 21 \end{pmatrix}$

- (b) (12 points) Explain how to cryptanalyze this cipher using a known plaintext attack.

Solution: The attack is similar to the attack on the usual Hill cipher. Suppose

4261 Midterm (continued)

n is the dimension of the matrix and that $n + 1$ plaintexts x_i with corresponding ciphertexts y_i have been found with the additional requirement that the difference of first n plaintexts with the last form the columns of an invertible mod-26 matrix. So we have equations of the form: $Mx_1 + v = y_1, Mx_2 + v = y_2, \dots, Mx_n + v = y_n, Mx_{n+1} + v = y_{n+1}$. Subtracting the last equation from the i 'th we get $M(x_i - x_{n+1}) = y_i - y_{n+1}, M(x_2 - x_{n+1}) = y_2 - y_{n+1}, \dots, M(x_n - x_{n+1}) = y_n - y_{n+1}$. Letting

$$A = \begin{pmatrix} \vdots & \vdots & & \vdots \\ x_1 - x_{n+1} & x_2 - x_{n+1} & \dots & x_n - x_{n+1} \\ \vdots & \vdots & & \vdots \end{pmatrix}$$

and

$$B = \begin{pmatrix} \vdots & \vdots & & \vdots \\ y_1 - y_{n+1} & y_2 - y_{n+1} & \dots & y_n - y_{n+1} \\ \vdots & \vdots & & \vdots \end{pmatrix}$$

the previous system of equations is just $MA = B$. Furthermore, by assumption A is invertible (and with enough known plaintexts, we expect to find such an A) so we can multiply both sides by A^{-1} obtaining $M = BA^{-1}$. To resolve the final part of the key, v , solve for v in $Mx_1 + v = y_1$ to get $v = y_1 - Mx_1$.