550.371 Cryptology and Coding, Exam 1, Spring 2016

In proving any result, you may cite and use any logically preceding results without proof. Blank answers will be awarded 20% credit, but no credit will be given for answers without basic merit.

Problem 1: (10 points) Prove the Fundamental Theorem of Arithmetic. Specifically, that every positive integer’s prime factorization is unique (up to re-ordering of the primes).

Solution: By way of contradiction, suppose this is not the case, and there exists a positive integer with more than one prime factorization. Let \( n \) be the smallest positive integer with more than one factorization, and say they are \( n = \prod_{i=1}^{r} p_i \) and \( n = \prod_{j=1}^{s} q_j \). Clearly \( n > 1 \). Now, \( p_1 | \prod_{j=1}^{s} q_j \); that is to say \( p_1 \prod_{j=1}^{s} q_j \) thus, by a lemma from lecture, \( p_1 = q_{j^*} \) for some \( j^* \) among \( 1, 2, \ldots, s \). Thus we have two different prime factorizations for \( \prod_{i=2}^{r} p_i = \prod_{j=1,j\neq j^*}^{s} q_j \), which is less than \( n \), contradicting the minimality of \( n \). Thus there are no counterexamples, and the result is shown.

Problem 2: (10 points) Let \( a, b \) be integers. Prove that \( \gcd(a, b) = 1 \) if and only if there exist integers \( x, y \) such that \( xa + yb = 1 \). (Be very, very clear on the \( \Leftarrow \) direction.)

Solution: By a theorem from lecture, we have \( \gcd(a, b) = \min\{xa + yb : x, y \in \mathbb{Z}, xa + by > 0\} \). Thus, if \( \gcd(a, b) = 1 \), we have existence of integers \( x, y \) such that \( xa + yb = \gcd(a, b) = 1 \). Conversely, if there exists integers \( x, y \) such that \( xa + yb = 1 \) then, since 1 is the minimum positive integer, we have that \( 1 = \min\{xa + yb : x, y \in \mathbb{Z}, xa + by > 0\} = \gcd(a, b) \), as desired.
Problem 3: (10 points) Suppose plaintexts $m_1, m_2, m_3, \ldots \in \mathbb{Z}_2^r$ are to be sent from Alice to Bob, and the encryption function is $E_e(\cdot)$, and the decryption function is $D_d(\cdot)$. Diagram cipherblock chaining mode, and show that the plaintexts are indeed recovered by Bob.

Problem 4: (10 points) Suppose that $X$ and $Y$ are independent random letters from the English corpus; so, for each $i = 0, 1, 2, \ldots, 25$, it holds that $P(X = i) = P(Y = i) = \mu_i$. Write a statement involving probability, $X$, and $Y$ that is critical to the successful attack on the Vigenere cipher.

Solution: The statement is that, for all $\tau \in \{0, 1, 2, \ldots, 25\}$,

$$P(X + \tau = Y \mod 26) = \begin{cases} .066 & \text{if } \tau = 0 \\ < .045 & \text{if } \tau \neq 0 \end{cases}$$

Problem 5: (10 points) Write down the three concerns with symmetric cryptosystems which we identified in lecture (and which will not be concerns with public key cryptosystems).
Problem 6: (10 points) In DES, Alice computes the ciphertext $c \in \mathbb{Z}_2^{64}$ from the plaintext $m \in \mathbb{Z}_2^{64}$ by evaluating $c := \text{DES}_K(m)$, where $K \in \mathbb{Z}_2^{64}$ is the DES key. Assume Eve has a very fast computer and, if she discovers a known plaintext $m$ and its corresponding ciphertext $c$, then she can try all $2^{64}$ DES keys in $\mathbb{Z}_2^{64}$ until she finds the right $K$ that encrypts $c = \text{DES}_K(m)$.

Knowing this, Alice and Bob agree on two keys $K, L \in \mathbb{Z}_2^{64}$ and they agree that Alice will instead encrypt $c := \text{DES}_K(m + L)$, where $+$ denotes mod 2 addition. Show how, with two known-plaintexts $m_1, m_2$ and their corresponding ciphertexts $c_1, c_2$, Eve can indeed find the pair of keys.

Solution: Suppose $c_1 = \text{DES}_K(m_1 + L)$ and $c_2 = \text{DES}_K(m_2 + L)$. Recall that the decryption of DES is precisely the encryption of DES with reversal of order in round keys “$\overline{K}$”. Thus taking $\text{DES}_{\overline{K}}(\cdot)$ of both sides yields $\text{DES}_{\overline{K}}(c_1) = m_1 + L$ and $\text{DES}_{\overline{K}}(c_2) = m_2 + L$, which means that $m_1 = \text{DES}_{\overline{K}}(c_1) + L$ and $m_2 = \text{DES}_{\overline{K}}(c_2) + L$; adding, we get $m_1 + m_2 = \text{DES}_{\overline{K}}(c_1) + \text{DES}_{\overline{K}}(c_2)$ from which Eve can get $K$ by trying all $2^{64}$ possibilities, then Eve computes $L$ as $m_1 + \text{DES}_{\overline{K}}(c_1)$.

Problem 7: (10 points) Consider the algorithm for testing the primality of positive integer $a$, which checks each of $d = 2, 3, 4, \ldots, \sqrt{a}$ to see if $d | a$, returning “composite” or “prime” according as $d | a$ for one of these $d$ (or $d \not| a$ for all of these $d$). Carefully and clearly check the criterion for efficiency to decide if this algorithm is efficient or not.

Solution: Here $x := \text{size of instance} = \Theta \log a$. (The base of log will be 2 for now.)

The running time is $\Theta \left[a^{1/2}\right] = \Theta \left[(2^{\log a})^{1/2}\right] = \Theta \left[2^{\frac{1}{2} \log a}\right] = \Theta \left[\sqrt{2}^{\log a}\right] = \Theta \left[\sqrt{2}^x\right]$, which is exponential in the size of the instance. Thus the algorithm is not efficient, since this exponential function grows faster than any polynomial.
SCRAP PAPER This page will not be graded.