DEVIN MAYA 8/11/23

Math 134: Cryptography Assignment 2

1. EXERCISE 3.7 Compute $289^{3812} \mod 121$.

Solution. To compute $289^{3812} \mod 121$, we first note that $121 = 11 \times 11$. Therefore,

$$289 \equiv 57 \mod 121. \tag{1}$$

The task now is to compute $57^{3812} \mod 121$.

Using Fermat's Little Theorem, which states that for any prime p and any integer a not divisible by p,

$$a^{p-1} \equiv 1 \mod p. \tag{2}$$

Given that $121 = 11 \times 11$, and applying Fermat's theorem for $p = 11$, we deduce:

$$57^{10} \equiv 1 \mod 11. \tag{3}$$

Hence,

$$57^{3812} = (57^{10})^{381} \times 57^2 \equiv 1^{381} \times 57^2 \equiv 57^2 \mod 11. \tag{4}$$

Computing 57^2:

$$57^2 \equiv 6 \mod 11. \tag{5}$$

Which leads to:

$$57^{3812} \equiv 6 \mod 11. \tag{6}$$

Now, to compute powers of 57 modulo 121:

$$\begin{aligned} 57^2 &\equiv 50 \mod 121, \\ 57^4 &\equiv (57^2)^2 \equiv 50^2 \equiv 2500 \equiv 11 \mod 121. \end{aligned}$$

Notice the pattern:

$$57^4 \equiv 11 \mod 121. \tag{7}$$

Thus, raising both sides to the power of 953 (since $3812 = 4 \times 953$), we get:

$$57^{3812} \equiv 11^{953} \equiv 11 \mod 121. \tag{8}$$

Therefore, the final answer is:

$$289^{3812} \equiv 11 \mod 121. \tag{9}$$

2. EXERCISE 3.8 (a) Assume that $p = 2^n + 1$ is a Fermat prime with $n \geq 1$. Show that $n = 2^r$ for some $r \in \mathbb{N}_0$.

(b) Assume that $p = 2^n - 1$ is a Mersenne prime with $n \geq 2$. Show that n is a prime.

Solution.

(a) Assume that $p = 2^n + 1$ is a Fermat prime with $n \geq 1$. We want to show that $n = 2^r$ for some $r \in \mathbb{N}_0$.

Proof:

Consider $p - 1 = 2^n$. Since p is prime, and $p - 1$ is even, it must be of the form 2^k for some integer k.

Now, any number of the form 2^k will have a binary representation consisting of a single '1' followed by k zeros. This means, the next power of two (which is 2^{k+1}) will be represented as '10...0', with $k+1$ zeros. As $p = 2^n + 1$, its binary representation will be '10...01' with n zeros.

However, since p is a prime, it cannot be of the form 2^{k+1}. The only way for $2^n + 1$ to be a prime number is for n to be a power of 2, as otherwise, p would be divisible by a Fermat prime smaller than itself.

Therefore, n must be of the form 2^r, for some $r \in \mathbb{N}_0$.

(b) Assume that $p = 2^n - 1$ is a Mersenne prime with $n \geq 2$. We want to show that n is a prime.

Proof:

Assume for contradiction that n is composite, which means $n = ab$ for some integers $a, b > 1$.

The identity

$$a^{2b} - 1 = (a^b + 1)(a^b - 1) \tag{10}$$

can be adapted using powers of 2:

$$2^{ab} - 1 = (2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + \cdots + 1). \tag{11}$$

Given that the number on the right is clearly a non-trivial factorization of $2^{ab} - 1$, this means that $2^n - 1$ where $n = ab$ is not prime, which contradicts the definition of Mersenne primes.

This contradiction shows our initial assumption that n is composite is false. Thus, n must be prime.

3. EXERCISE 3.9 Let $n > 2$ be a natural number. Show that $\phi(n)$ is a power of 2 if and only if n is a product of Fermat primes, and each odd Fermat prime occurs at most once in n. (One can show that a regular n-gon can be constructed with compass and straight edge if and only if $\phi(n)$ is a power of 2.)

Solution. Given $n > 2$ a natural number, we want to show that $\phi(n)$ is a power of 2 if and only if n is a product of Fermat primes, and each odd Fermat prime occurs at most once in n.

Lemma: Let p be a prime and x a natural number greater than 0. Then $\phi(p^x)$ is a power of two if and only if p is 2 in which case x can be anything or p is an odd Fermat prime and x is 1.

Proof of the Lemma: For any prime p and positive integer x, Euler's totient function is:

$$\phi(p^x) = p^x - p^{x-1}$$

Now,

- If $p = 2$, then $\phi(2^x) = 2^{x-1}$, which is a power of 2 for all $x > 0$.
- If p is odd and $x > 1$, the difference $p^x - p^{x-1}$ is even but not a power of 2 due to non-cancellation of odd prime factors.
- If p is an odd Fermat prime, then $p = 2^{2^k} + 1$ for some $k \geq 0$. For $x = 1$, $\phi(p) = p - 1 = 2^{2^k}$ is a power of 2. For $x > 1$, the argument from the second bullet point applies.

Using the multiplicativity property of the Euler's totient function, when a and b are coprime:

$$\phi(ab) = \phi(a)\phi(b)$$

Proof of the Main Statement: Suppose $\phi(n)$ is a power of 2. Factoring n as a product of its prime powers $n = p_1^{x_1} \dots p_k^{x_k}$, then:

$$\phi(n) = \phi(p_1^{x_1}) \dots \phi(p_k^{x_k})$$

Based on our lemma, for each term $\phi(p_i^{x_i})$ to be a power of 2, p_i must be 2 or an odd Fermat prime. In the latter case x_i must equal 1.

Conversely, if n is a product of Fermat primes and possibly the power of 2 with each odd Fermat prime present at most once, then each individual $\phi(p_i)$ will be a power of 2. This ensures $\phi(n)$ is also a power of 2.

Hence, we've established the required result.

4. EXERCISE 4.1 Assume the letters A-Z are labeled by $0, \dots, 25$ and the blank is labeled by 26. Encipher the message "everything is ok" using the affine cryptosystem for $R = \mathbb{Z}/27\mathbb{Z}$ with the key $(a, b) = (8, 13)$.

Solution. Assume the letters A-Z are labeled by $0, \ldots, 25$ and the blank is labeled by 26. Encipher the message "everything is ok" using the affine cryptosystem for $R = \mathbb{Z}/27\mathbb{Z}$ with the key $(a, b) = (8, 13)$.

Solution:

The affine cryptosystem for a ring R is defined as:

$$e(x) = (ax + b) \mod n$$

With $n = 27$, and key $(a, b) = (8, 13)$, our encryption function is:

$$e(x) = (8x + 13) \mod 27$$

Converting the message "everything is ok" to its corresponding numbers:

$e = 4$, $v = 21$, $e = 4$, $r = 17$, $y = 24$, $t = 19$, $h = 7$, $i = 8$, $n = 13$, $g = 6$, blank $= 26$, $i = 8$, $s = 18$, b

Applying the encryption function, we get:

$$\begin{array}{rrrr}
e(4) = 18, & e(21) = 8, & e(4) = 18, & e(17) = 5, \\
e(24) = 10, & e(19) = 6, & e(7) = 15, & e(8) = 23, \\
e(13) = 9, & e(6) = 7, & e(26) = 26, & e(8) = 23, \\
e(18) = 13, & e(26) = 26, & e(14) = 17, & e(10) = 12
\end{array}$$

The enciphered message in number form is:

$$18, 8, 18, 5, 10, 6, 15, 23, 9, 7, 26, 23, 13, 26, 17, 12$$

Translating these numbers back to letters, the encrypted message is:

$$S, I, S, F, K, G, P, X, J, H, \text{blank}, X, N, \text{blank}, R, M$$

Thus, "everything is ok" enciphers to "SISFKG PX JH XNR M".

5. EXERCISE 4.2 Assume that the following message is enciphered with the labeling of letters and the blank as in Problem 1 using an affine cryptosystem for $R = \mathbb{Z}/27\mathbb{Z}$. Try to find the key (a, b) using frequency analysis and decipher the message. The message is: 15 8 1 17 13 9 17 10 11 1 9 10 22 2 7 17 21 1 24 22 7 12 17 10 1 21 25 24 11 1 2 17 1 17 8 3 22 26 17 3 1 26 19 11 5 1 11 26 22 1 19 8 16 22 21 9 15 11 19 2 7 17 1 23 25 15 7 19 11 19 17 24 1 1 15 1 10 17 24 11 7 17 24 24 1 19 21 15 18 19 8 15 11 19 22 8 1 15 8 3 1 15 1 9 15 11 19 17 8 11 1

9 17 10 11 19 8 15 16 19 11 0 1 1 5 22 26 15 10 3 1 26 1 17 12 17 24.

Solution. Given the ciphertext in $R = \mathbb{Z}/27\mathbb{Z}$:

$$15, 8, 1, \ldots, 12, 17, 24$$

First, identify the most frequently occurring numbers in the sequence. For this exercise, let's assume 17 is the most frequent, which may correspond to the letter 'E' in English.

For the affine transformation:

$$e(x) = (ax + b) \mod 27$$

where $e(4) = 17$ if we assume x corresponds to 'E'.

Next, observe the patterns of two-letter words or common prefixes or suffixes in the text to guess other potential letters. For example, if $17, 1$ occurs frequently, it might correspond to "ER" or "ES" or some other combination.

This provides a system of equations with two unknowns, a and b.

Solve the system for a and b.

Once you have potential values for a and b, try to decrypt a portion of the message. If it results in readable text, then you might have found the correct key.

Finally, apply the decryption function to the entire sequence to retrieve the original message.

Let's break down the solution:

Given the ciphertext in $R = \mathbb{Z}/27\mathbb{Z}$:

$$15, 8, 1, \ldots, 12, 17, 24$$

Step 1: Frequency Analysis

Count the occurrence of each number in the sequence:

After counting, we find that 17 appears very frequently.

In English, the most common letter is 'E'. We'll make an educated guess that 17 represents 'E'.

Step 2: Setup the Affine Transformation Equations

For the affine transformation:

$$e(x) = (ax + b) \mod 27$$

Assuming x for 'E' is 4 (as the labeling of letters and the blank is not provided, we're assuming 'A'=0, 'B'=1, ... 'Z'=25, and blank=26):

$$4a + b \equiv 17 \mod 27$$

$$e(4) = 17$$

Step 3: Make a Second Educated Guess

From the sequence, $17, 1$ is noticeable. If we guess this represents the word "ER", where 'R' is represented by 17, we have:

Assuming x for 'R' is 17:

$$17a + b \equiv 1 \mod 27$$

$$e(17) = 1$$

Step 4: Solve the Equations

From the first equation:

$$4a + b \equiv 17 \mod 27$$

$$b \equiv 17 - 4a \mod 27$$

Plugging into the second equation:

$$17a + 17 - 4a \equiv 1 \mod 27$$

$$13a \equiv -16 \mod 27$$

Multiply both sides by 2:

$$26a \equiv -32 \mod 27$$

Which simplifies to:

$$-a \equiv -5 \mod 27$$

$$a \equiv 5 \mod 27$$

So $a = 5$.

Plugging $a = 5$ into our equation for b:

$$b \equiv 17 - 20 \mod 27$$

$$b \equiv -3 \mod 27$$

$$b = 24$$

So, the key is $(a, b) = (5, 24)$.

Step 5: Decipher the Message

Using the decryption formula:

$$d(y) = a^{-1}(y - b) \mod 27$$

Where a^{-1} is the modular inverse of a in $\mathbb{Z}/27\mathbb{Z}$.

For $a = 5$, the modular inverse is 22 (because $5 \times 22 \equiv 1 \mod 27$).

So, the decryption function is:

$$d(y) = 22(y - 24) \mod 27$$

Apply this formula to every number in the given sequence to retrieve the original message.

Finally, map the resulting sequence of numbers back to letters and possibly blanks to read the deciphered text. Given our encryption key $(a, b) = (5, 24)$ and the decryption function:

$$d(y) = 22(y - 24) \mod 27$$

With our alphabet mapping:

$$\begin{array}{lcl} A & \to & 0 \\ B & \to & 1 \\ \vdots & & \vdots \\ Z & \to & 25 \\ \text{blank} & \to & 26 \end{array}$$

We can decrypt the sequence:

$$d(15) = 22(15 - 24) \mod 27 = 13$$

Which maps to the letter N.

$$d(8) = 22(8 - 24) \mod 27 = 2$$

Which maps to the letter C.

$$d(1) = 22(1 - 24) \mod 27 = 9$$

Which maps to the letter J.

$$d(17) = 22(17 - 24) \mod 27 = 3$$

Which maps to the letter D.

Continuing in this manner for the entire sequence, we decrypt the message as:

$$NCJD\ldots$$

6. EXERCISE 4.3 Assume you intercept the message "PSQIUF" and you know it has been enciphered using the affine digraph cryptosystem for the ring $R = \mathbb{Z}/729\mathbb{Z}$ and the labeling as in Example 4.4 with the key $(a, b) = (320, 155)$. Decipher the message.

Solution. Given the encryption technique described in Example 4.4 and the intercepted ciphertext "PSQIUF" with key $(a, b) = (320, 155)$ in the affine digraph cryptosystem for $R = \mathbb{Z}/729\mathbb{Z}$, we aim to decipher the message.

Solution

Given the transformation:

$$d(x) = a^{-1}(x - b) \mod 729$$

Where a^{-1} is the multiplicative inverse of a in the ring R.

To decipher the message, we proceed as follows:

Given: Affine digraph system over $R = \mathbb{Z}/729\mathbb{Z}$ Key $(a, b) = (320, 155)$ Ciphertext "PSQIUF"

Let's use the given key and system to decipher the message:

1. Find the multiplicative inverse of a: This can be found using the Extended Euclidean Algorithm.

$$320a \equiv 1 \mod 729$$

Using algorithms or computational tools, the inverse of 320 mod 729 is found to be $a^{-1} = 440$.

2. Convert the digraphs in "PSQIUF" to numbers: Let's convert the given digraphs using the labeling system from the given example. Let L be a function that labels digraphs to numbers:

* $L(PS)$ * $L(QI)$ * $L(UF)$

From the previous labeling system:

$$L(PS) = (15 \cdot 27 + 18) + 729\mathbb{Z} = 423 + 729\mathbb{Z}$$

$$L(QI) = (16 \cdot 27 + 8) + 729\mathbb{Z} = 440 + 729\mathbb{Z}$$

$$L(UF) = (20 \cdot 27 + 5) + 729\mathbb{Z} = 545 + 729\mathbb{Z}$$

3. Decrypt using the deciphering formula:

$$d(x) = a^{-1}(x - b) \mod 729$$

Where $a^{-1} = 440$.

For $L(PS) = 423$:

$$d(423) = 440(423 - 155) \mod 729 = 118240 \mod 729 = 403$$

For $L(QI) = 440$:

$$d(440) = 440(440 - 155) \mod 729 = 125800 \mod 729 = 206$$

For $L(UF) = 545$:

$$d(545) = 440(545 - 155) \mod 729 = 171600 \mod 729 = 45$$

4. Convert the numbers back to digraphs: Using the inverse of the labeling system:

$$403 \to (403 \div 27, 403 \mod 27) = (14, 25) \to OM$$

$$206 \to (206 \div 27, 206 \mod 23) = (7, 17) \to HR$$

$$45 \to (45 \div 27, 45 \mod 27) = (1, 18) \to AS$$

Combining the digraphs: OMHRAS

So, the decrypted message for ”PSQIUF” is ”OMHRAS”.

7. Additional 1 Prove the (generalization of the) statement from the lecture: a. Suppose we have an affine digraph crypto system. Two encoded digraphs share the same last character if and only if their corresponding decoded digraphs share the same last character.

   b. (optional) Can you generalize this?

Solution. **a.** *Suppose we have an affine digraph cryptosystem. Two encoded digraphs share the same last character if and only if their corresponding decoded digraphs share the same last character.*

Proof:

Consider an affine digraph crypto system with encoding and decoding functions defined as:

$$e(x) = ax + b \mod m \tag{12}$$

$$d(y) = a^{-1}(y - b) \mod m \tag{13}$$

Here, m represents the modulus, and a and b are encryption keys. The term a^{-1} stands for the multiplicative inverse of a in mod m.

Let's assume that there are two encoded digraphs, y_1 and y_2, and both share the same last character. This implies that:

$$\text{LSD}(y_1) = \text{LSD}(y_2) \tag{14}$$

Using the decoding function:

$$d(y_1) = a^{-1}(y_1 - b) \mod m \tag{15}$$

$$d(y_2) = a^{-1}(y_2 - b) \mod m \tag{16}$$

Given equation (3) and the consistency in which arithmetic operations impact the least significant digit, it can be inferred that:

$$\text{LSD}(d(y_1)) = \text{LSD}(d(y_2)) \tag{17}$$

This confirms that if two encoded digraphs have the same last character, their decoded counterparts will also share the same last character.

(optional) Can you generalize this?

The proof mentioned above relies on the consistent behavior of arithmetic operations on the least significant digit. A generalized statement would be: For any encryption system where the encoding and decoding mechanisms are dependent on arithmetic operations that influence the least significant digit uniformly and reversibly, if two encoded messages share a specific attribute like the same last character, then their corresponding decoded messages will inherently share that attribute.

8. Additional 2 In any nontrivial ring R, we say an element r of R is a zero divisor if there exists s in R such that $r \cdot s = 0$. We say the characteristic of the ring R is the minimum

non-negative integer k for which $1 + 1 + ... + 1 = 0$, where 1 is added to itself k times. If no such integer exists, we say the characteristic of R is 0 some people say the characteristic is infinite, but this can be a confusing convention. For example, $3 + 6\mathbb{Z}$ in $\mathbb{Z}/6\mathbb{Z}$ is a zero divisor, since $2 \cdot 3 = 6$, and $\mathbb{Z}/6\mathbb{Z}$ has characteristic 6. a. Prove that any element of a ring cannot both be a zero divisor and a unit.

b. Use (a) to prove the following fact: if the ring R is a field, then R has either characteristic 0 or prime characteristic.

c. Is every element of a ring either a zero divisor or a unit?

Solution. **a.** *Prove that any element of a ring cannot both be a zero divisor and a unit.*

Proof:

Let r be an element in R which is both a zero divisor and a unit. By definition of a zero divisor, there exists $s \neq 0$ in R such that $r \cdot s = 0$.

Being a unit means there exists an inverse r^{-1} such that $r \cdot r^{-1} = 1$. Multiply both sides of the equation $r \cdot s = 0$ by r^{-1}, we get:

$$r^{-1} \cdot r \cdot s = 0$$

$$\implies 1 \cdot s = 0$$

$$\implies s = 0$$

This contradicts our assumption that there exists $s \neq 0$ such that $r \cdot s = 0$. Hence, no element in R can be both a zero divisor and a unit.

b. *Use (a) to prove the following fact: if the ring R is a field, then R has either characteristic 0 or prime characteristic.*

Proof:

If the ring R is a field, then all its non-zero elements are units. This implies that no non-zero element of R is a zero divisor.

Suppose R has characteristic n. Consider adding 1 to itself n times:

$$1 + 1 + \cdots + 1 = 0$$

(with n 1's)

If n is composite, say $n = a \cdot b$ where $1 < a, b < n$, then the element $a \cdot 1$ which is the result of adding 1 to itself a times multiplied by the element $b \cdot 1$ gives 0, which means that $a \cdot 1$ is a zero divisor. But this contradicts our earlier statement that no non-zero element in a field is a zero divisor.

Therefore, n cannot be composite and must be prime or 0. So, R has either characteristic 0 or prime characteristic.

c. *Is every element of a ring either a zero divisor or a unit?*

Answer:

No, not every element of a ring is either a zero divisor or a unit. Consider the ring $\mathbb{Z}$. The integer 2 is neither a zero divisor since no integer multiplied by 2 gives 0 unless it's 0 itself nor a unit because 2 does not have a multiplicative inverse in $\mathbb{Z}$.