SOLVING CONGRUENCE

CH.4.4 DISCRETE MATHEMATICS ROSEN

THEOREM 4.4.4: FERMAT'S LITTLE THEOREM AND MODULAR EXPONENTIATION

- If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$
- Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$
- Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.
- **Example**: Find 7^{222} **mod** 11.
- By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$, for every positive integer k. Therefore,
- $7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}$.
- Hence, 7^{222} **mod** $11 = 5$.

PROOF OF CLAIM

- Claim: if $a = b(mod\ m)$, then $a^k = b^k(mod\ m)$
- Proof: (base step) for $k = 1 \rightarrow a = b(mod\ m)$ true by assumption
- Inductive step: Assume true for k
- $a^{k+1} = b^{k+1}(mod\ m) = a^k * a = b^k(mod\ m)b(mod\ m)$
- $a^k * b(mod\ m) = b^k(mod\ m)b(mod\ m) \rightarrow a^k = b^k(mod\ m)$

EXAMPLE 4

- Use Fermat's Little Theorem to help you find the following:
- $7^{121}(mod\ 13)$
  - Note: $7^{12} = 1(mod\ 13) \rightarrow 7^{120} = 1(mod\ 13)$
  - $7^{121} = 7 * 1(mod\ 13) = 7(mod\ 13) = 7$
- $5^{2023}(mod\ 7)$
  - Note: $5^{6} = 1(mod\ 7) \rightarrow 5^{1998} = 1(mod\ 7)$
  - $5^{2023} = 5^{5}(mod\ 7) = (5^{3} mod\ 7)(5^{2} mod\ 7) mod\ 7 = 6 * 4 mod\ 7 = 24 mod\ 7 = 3$

CRYPTOGRAPHY

CH.4.6 DISCRETE MATHEMATICS ROSEN

CAESAR CIPHER

Julius Caesar created secret messages by shifting each letter three letters forward in the alphabet (sending the last three letters to the first three letters.) For example, the letter B is replaced by E and the letter X is replaced by A. This process of making a message secret is an example of *encryption*.

Here is how the encryption process works:

- Replace each letter by an integer from $\mathbf{Z}_{26}$, that is an integer from 0 to 25 representing one less than its position in the alphabet.
- The encryption function is $f(p) = (p + 3) \bmod 26$. It replaces each integer p in the set $\{0,1,2,...,25\}$ by $f(p)$ in the set $\{0,1,2,...,25\}$.
- Replace each integer p by the letter with the position $p + 1$ in the alphabet.

Example: Encrypt the message "MEET YOU IN THE PARK" using the Caesar cipher.

Solution: 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3) \bmod 26$.

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

Translating the numbers back to letters produces the encrypted message

"PHHW BRX LQ WKH SDUN."

CAESAR CIPHER

- To recover the original message, use $f^{-1}(p) = (p-3) \bmod 26$. So, each letter in the coded message is shifted back three letters in the alphabet, with the first three letters sent to the last three letters. This process of recovering the original message from the encrypted message is called *decryption*.
- The Caesar cipher is one of a family of ciphers called *shift ciphers*. Letters can be shifted by an integer k, with 3 being just one possibility. The encryption function is

  $$f(p) = (p + k) \bmod 26$$

  and the decryption function is

  $$f^{-1}(p) = (p-k) \bmod 26$$

  The integer k is called a *key*.

CRYPTOSYSTEM I | SHIFT CIPHER

	Encryption	Decryption	Key
i. Basic	$f(c) = x + k \ mod\ 26$	$f^{-1}(y) = y - k \ mod\ 26$	K-shift
ii. Affine Transformation	$f(c) = ax + k \ mod\ 26$	$f^{-1}(y) = \bar{a}y - k \ mod\ 26$	(a.k)

EXAMPLE 1

Encrypt the message "STOP GLOBAL WARMING" using the shift cipher with $k = 11$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

$$18\ 19\ 14\ 15 \quad 6\ 11\ 14\ 1\ 0\ 11 \quad 22\ 0\ 17\ 12\ 8\ 13\ 6.$$

Apply the shift $f(p) = (p + 11)$ **mod** 26, yielding

$$3\ 4\ 25\ 0 \quad 17\ 22\ 25\ 12\ 11\ 22 \quad 7\ 11\ 2\ 23\ 19\ 24\ 17.$$

Translating the numbers back to letters produces the ciphertext

"DEZA RWZMLW HLCXTYR."

EXAMPLE 2

Decrypt the message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted using the shift cipher with $k = 7$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

$$11\ 4\ 22\ 11\ 24\ 15\ 11\ 20\ 9\ 11 \quad 15\ 25 \quad 7 \quad 13\ 24\ 11\ 7 \quad 0 \quad 0\ 11\ 7 \quad 9 \quad 14 \quad 11 \quad 24.$$

Shift each of the numbers by $-k = -7$ modulo 26, yielding

$$4\ 23\ 15\ 4\ 17\ 8\ 4\ 13\ 2\ 4 \quad 8\ 18 \quad 0 \quad 6\ 17\ 4 \quad 0 \quad 19 \quad 19 \quad 4 \quad 0 \quad 2 \quad 7 \quad 4 \quad 17.$$

Translating the numbers back to letters produces the decrypted message

"EXPERIENCE IS A GREAT TEACHER."

CRYPTOANALYSIS

- Question: What if you don't have a key?
- Cryptoanalysis (code breaking) of a basic shift cipher
- **Method 1.** Brute Force: check each possible shift (26 total)
- **Method 2.** Letter Frequencies: (i.e Brute Force with a preference)

CRYPTOANALYSIS: LETTER FREQUENCIES

1. Count the number of items each letter appears in the cipher text
2. Hypothesize that the most frequent letter is E (This letter appears the most in the English Language)
3. Determine k under the hypothesis
4. Attempt to decipher
5. if it tails continue main assumptions for the letter T...

- Note: Shift Ciphers are extremely each to break (not reliable)

CRYPTOSYSTEM II | BLOCK CIPHER

- Ciphers that replace each letter of the alphabet by another letter are called *character* or *monoalphabetic* ciphers.
- They are vulnerable to cryptanalysis based on letter frequency. *Block ciphers* avoid this problem, by replacing blocks of letters with other blocks of letters.
- A simple type of block cipher is called the *transposition cipher*. The key is a permutation σ of the set $\{1,2,\ldots,m\}$, where m is an integer, that is a one-to-one function from $\{1,2,\ldots,m\}$ to itself.
- To encrypt a message, split the letters into blocks of size m, adding additional letters to fill out the final block. We encrypt $p_1,p_2,\ldots,p_m$ as $c_1,c_2,\ldots,c_m = p_{\sigma(1)},p_{\sigma(2)},\ldots,p_{\sigma(m)}$.
- To decrypt the $c_1,c_2,\ldots,c_m$ transpose the letters using the inverse permutation σ^{-1}.

EXAMPLE 3

Example: Using the transposition cipher based on the permutation σ of the set $\{1,2,3,4\}$ with $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 2,$

a. Encrypt the plaintext PIRATE ATTACK

b. Decrypt the ciphertext message SWUE TRAEOEHS, which was encryted using the same cipher.

Solution:

a. Split into four blocks PIRA TEAT TACK.

Apply the permutation σ giving IAPR ETTA AKTC.

b. σ^{-1}: $\sigma^{-1}(1) = 2, \sigma^{-1}(2) = 4, \sigma^{-1}(3) = 1, \sigma^{-1}(4) = 3.$

Apply the permutation σ^{-1} giving USEW ATER HOSE.

Split into words to obtain USE WATER HOSE.

CRYPTOGRAPHY

CH.4.6 DISCRETE MATHEMATICS ROSEN

EXAMPLE 2

Decrypt the message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted using the shift cipher with $k = 7$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

$$11\ 4\ 22\ 11\ 24\ 15\ 11\ 20\ 9\ 11 \quad 15\ 25 \quad 7 \quad 13\ 24\ 11\ 7 \quad 0 \quad 0\ 11\ 7 \quad 9 \quad 14 \quad 11 \quad 24.$$

Shift each of the numbers by $-k = -7$ modulo 26, yielding

$$4\ 23\ 15\ 4\ 17\ 8\ 4\ 13\ 2\ 4 \quad 8\ 18 \quad 0 \quad 6\ 17\ 4 \quad 0 \quad 19 \quad 19 \quad 4 \quad 0 \quad 2 \quad 7 \quad 4 \quad 17.$$

Translating the numbers back to letters produces the decrypted message

"EXPERIENCE IS A GREAT TEACHER."

CRYPTOANALYSIS

- Question: What if you don't have a key?
- Cryptoanalysis (code breaking) of a basic shift cipher
- **Method 1.** Brute Force: check each possible shift (26 total)
- **Method 2.** Letter Frequencies: (i.e Brute Force with a preference)

CRYPTOANALYSIS: LETTER FREQUENCIES

1. Count the number of items each letter appears in the cipher text
2. Hypothesize that the most frequent letter is E (This letter appears the most in the English Language)
3. Determine k under the hypothesis
4. Attempt to decipher
5. if it fails continue main assumptions for the letter T...

- Note: Shift Ciphers are extremely each to break (not reliable)

CRYPTOSYSTEM II | BLOCK CIPHER

- Ciphers that replace each letter of the alphabet by another letter are called *character* or *monoalphabetic* ciphers.
- They are vulnerable to cryptanalysis based on letter frequency. *Block ciphers* avoid this problem, by replacing blocks of letters with other blocks of letters.
- A simple type of block cipher is called the *transposition cipher*. The key is a permutation σ of the set $\{1,2,\ldots,m\}$, where m is an integer, that is a one-to-one function from $\{1,2,\ldots,m\}$ to itself.
- To encrypt a message, split the letters into blocks of size m, adding additional letters to fill out the final block. We encrypt $p_1,p_2,\ldots,p_m$ as $c_1,c_2,\ldots,c_m = p_{\sigma(1)},p_{\sigma(2)},\ldots,p_{\sigma(m)}$.
- To decrypt the $c_1,c_2,\ldots,c_m$ transpose the letters using the inverse permutation σ^{-1}.

EXAMPLE 3

Using the transposition cipher based on the permutation σ of the set $\{1,2,3,4\}$ with $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 2$,

a. Encrypt the plaintext PIRATE ATTACK

b. Decrypt the ciphertext message SWUE TRAEOEHS, which was encryted using the same cipher.

Solution:

a. Split into four blocks PIRA TEAT TACK.

Apply the permutation σ giving IAPR ETTA AKTC.

b. σ^{-1}: $\sigma^{-1}(1) = 2, \sigma^{-1}(2) = 4, \sigma^{-1}(3) = 1, \sigma^{-1}(4) = 3.$

Apply the permutation σ^{-1} giving USEW ATER HOSE.

Split into words to obtain USE WATER HOSE.

CRYPTOSYSTEMS

Definition: A *cryptosystem* is a five-tuple $(\mathcal{P}, C, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where

- $\mathcal{P}$ is the set of plainntext strings,
- C is the set of ciphertext strings,
- $\mathcal{K}$ is the *keyspace* (set of all possible keys),
- $\mathcal{E}$ is the set of encryption functions, and
- $\mathcal{D}$ is the set of decryption functions.

- The encryption function in $\mathcal{E}$ corresponding to the key k is denoted by E_k and the decription function in $\mathcal{D}$ that decrypts cipher text enrypted using E_k is denoted by D_k. Therefore:

$$D_k(E_k(p)) = p, \text{ for all plaintext strings } p.$$

EXAMPLE 4

Describe the family of shift ciphers as a cryptosystem.

Solution: Assume the messages are strings consisting of elements in $\mathbf{Z}_{26}$.

- $\mathcal{P}$ is the set of strings of elements in $\mathbf{Z}_{26}$,
- C is the set of strings of elements in $\mathbf{Z}_{26}$,
- $\mathcal{K} = \mathbf{Z}_{26}$,
- $\mathcal{E}$ consists of functions of the form $E_k(p) = (p + k)$ **mod** 26 , and
- $\mathcal{D}$ is the same as $\mathcal{E}$ where $D_k(p) = (p - k)$ **mod** 26 .

PUBLIC KEY CRYPTOGRAPHY

- All classical ciphers, including shift and affine ciphers, are *private key cryptosystems*. Knowing the encryption key allows one to quickly determine the decryption key.
- All parties who wish to communicate using a private key cryptosystem must share the key and keep it a secret.
- In public key cryptosystems, first invented in the 1970s, knowing how to encrypt a message does not help one to decrypt the message. Therefore, everyone can have a publicly known encryption key. The only key that needs to be kept secret is the decryption key.

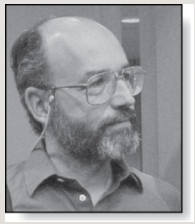
THE RSA CRYPTOSYSTEM

Clifford Cocks
(Born 1950)

- A public key cryptosystem, now known as the RSA system was introduced in 1976 by three researchers at MIT.

Ronald Rivest
(Born 1948)

Adi Shamir
(Born 1952)



Leonard
Adelman
(Born 1945)

- It is now known that the method was discovered earlier by Clifford Cocks, working secretly for the UK government.
- The public encryption key is (n,e), where $n = pq$ (the modulus) is the product of two large (200 digits) primes p and q, and an exponent e that is relatively prime to $(p-1)(q-1)$. The two large primes can be quickly found using probabilistic primality tests, discussed earlier. But $n = pq$, with approximately 400 digits, cannot be factored in a reasonable length of time.

RSA ENCRYPTION

- To encrypt a message using RSA using a key (n,e) :
  i. Translate the plaintext message M into sequences of two digit integers representing the letters. Use 00 for A, 01 for B, etc.
  ii. Concatenate the two digit integers into strings of digits.
  iii. Divide this string into equally sized blocks of $2N$ digits where $2N$ is the largest even number $2525...25$ with $2N$ digits that does not exceed n.
  iv. The plaintext message M is now a sequence of integers $m_1, m_2, \ldots, m_k$.
  v. Each block (an integer) is encrypted using the function $C = M^e \bmod n$.

EXAMPLE 5

Encrypt the message STOP using the RSA cryptosystem with key$(2537,13)$.

- $2537 = 43 \cdot 59$,
- $p = 43$ and $q = 59$ are primes and $\gcd(e,(p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$.

Solution: Translate the letters in STOP to their numerical equivalents 18 19 14 15.

- Divide into blocks of four digits (because $2525 < 2537 < 252525$) to obtain 1819 1415.
- Encrypt each block using the mapping $C = M^{13} \bmod 2537$.
- Since $1819^{13} \bmod 2537 = 2081$ and $1415^{13} \bmod 2537 = 2182$, the encrypted message is 2081 2182.

RSA DECRYPTION

- To decrypt a RSA ciphertext message, the decryption key *d*, an inverse of e modulo $(p-1)(q-1)$ is needed. The inverse exists since $\gcd(e,(p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$.
- With the decryption key *d*, we can decrypt each block with the computation $M = C^d \bmod p \cdot q$. (see *text for full derivation*)
- RSA works as a public key system since the only known method of finding *d* is based on a factorization of *n* into primes. There is currently no known feasible method for factoring large numbers into primes.

EXAMPLE 6

The message 0981 0461 is received. What is the decrypted message if it was encrypted using the RSA cipher from the previous example.

Solution: The message was encrypted with $n = 43 \cdot 59$ and exponent 13. An inverse of 13 modulo $42 \cdot 58 = 2436$ (*exercise* 2 *in Section* 4.4) is $d = 937$.

- To decrypt a block C, $M = C^{937} \bmod 2537$.
- Since $0981^{937} \bmod 2537 = 0704$ and $0461^{937} \bmod 2537 = 1115$, the decrypted message is 0704 1115. Translating back to English letters, the message is HELP.

CRYPTOGRAPHIC PROTOCOLS: KEY EXCHANGE

- *Cryptographic protocols* are exchanges of messages carried out by two or more parties to achieve a particular security goal.
- *Key exchange* is a protocol by which two parties can exchange a secret key over an insecure channel without having any past shared secret information. Here the *Diffe-Hellman key agreement protcol* is described by example.
  - i. Suppose that Alice and Bob want to share a common key.
  - ii. Alice and Bob agree to use a prime p and a primitive root a of p.
  - iii. Alice chooses a secret integer k_1 and sends a^{k1} **mod** p to Bob.
  - iv. Bob chooses a secret integer k_2 and sends a^{k2} **mod** p to Alice.
  - v. Alice computes $(a^{k2})^{k1}$ **mod** p.
  - vi. Bob computes $(a^{k1})^{k2}$ **mod** p

  At the end of the protocol, Alice and Bob have their shared key

  $$(a^{k2})^{k1} \textbf{ mod } p = (a^{k1})^{k2} \textbf{ mod } p.$$

- To find the secret information from the public information would require the adversary to find k_1 and k_2 from a^{k1} **mod** p and a^{k2} **mod** p respectively. This is an instance of the discrete logarithm problem, considered to be computationally infeasible when p and a are sufficiently large.

CRYPTOGRAPHIC PROTOCOLS: DIGITAL SIGNATURES

Adding a *digital signature* to a message is a way of ensuring the recipient that the message came from the purported sender.

- Suppose that Alice's RSA public key is (n,e) and her private key is d. Alice encrypts a plain text message x using $E_{(n,e)}(x) = x^d \bmod n$. She decrypts a ciphertext message y using $D_{(n,e)}(y) = y^d \bmod n$.
- Alice wants to send a message M so that everyone who receives the message knows that it came from her.
  1. She translates the message to numerical equivalents and splits into blocks, just as in RSA encryption.
  2. She then applies her decryption function $D_{(n,e)}$ to the blocks and sends the results to all intended recipients.
  3. The recipients apply Alice's encryption function and the result is the original plain text since $E_{(n,e)}(D_{(n,e)}(x)) = x$.

Everyone who receives the message can then be certain that it came from Alice.

EXAMPLE 7

Suppose Alice's RSA cryptosystem is the same as in the earlier example with key$(2537,13)$, $2537 = 43 \cdot 59$, $p = 43$ and $q = 59$ are primes and $\gcd(e,(p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$.

Her decryption key is d = 937.

She wants to send the message "MEET AT NOON" to her friends so that they can be certain that the message is from her.

Solution: Alice translates the message into blocks of digits $1204\ 0419\ 0019\ 1314\ 1413$.

1. She then applies her decryption transformation $D_{(2537,13)}(x) = x^{937} \bmod 2537$ to each block.
2. She finds (using her laptop, programming skills, and knowledge of discrete mathematics) that $1204^{937} \bmod 2537 = 817$, $419^{937} \bmod 2537 = 555$, $19^{937} \bmod 2537 = 1310$, $1314^{937} \bmod 2537 = 2173$, and $1413^{937} \bmod 2537 = 1026$.
3. She sends $0817\ 0555\ 1310\ 2173\ 1026$.

When one of her friends receive the message, they apply Alice's encryption transformation $E_{(2537,13)}$ to each block. They then obtain the original message which they translate back to English letters.