Exam one Review

Specific Topic Coverage

* Introduction to security
* Number systems and modular arithmetic
* Classic and modern symmetric cryptography
* Substitution cyphers:
* Ceasar (simple substitution)
* Keyword
* Vigenere
* Playfair
* One-time pad (including binary one-time pad)
* Transposition (permutation) ciphers:
* Rail Fence
* Columnar
* Block Ciphers:
* Hill
* DES (and general Feistel cipher structure)

Exam is problem-based similar to samples having to do with cyphers

Binary Arithmetic Overflow

Different rules for unsigned binary and two’s complement

For unsigned binary, overflow occurs when there is a carry past the most significant digit.

Example for 4 bit unsigned binary 1101 + 0100 = 10001

13+4 = 17 which is more than 4 bits can represent ( so overflow)

For two’s complement, overflow occurs only when adding two positive numbers produces a negative result, or when adding two negative numbers produces a positive result, and in no other cases.

Example for 4-bit two’s complement: 0101 + 0110 = 1011

Here we add 5 and 6 and get -5, so overflow has occurred even

Calculating Large Modulo Numbers

It is often easier to calculate by hand than to use a computer program

Use **Modulo reduction** to compute the value

7^93 mod 60 = [(((7^5 mod 60)^6 mod 60)^3 mod 60)(7^3 mod 60)] mod 60

Vigenere Cipher Shortcut

We do not need to use the Vigenere table to apply the vigenere cipher

We can use a shortcut that does the same thing

Let’s use the key “EASY” to encrypt “SOMEPLAINTEXT” using the vigenere cipher

Adds letter values

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S | O | M | E | P | L | A | I | N | T | E | X | T |
| E | A | S | Y | E | A | S | Y | E | A | S | Y | E |
| 18+4 | 14+0 | 12+18 | 4+24 | 15+4 | 11+0 | 0+18 | 8+24 | 13+4 | 19+0 | 4+18 | 23+24 | 19+4 |
| W | O | E | C | T | L | S | I | R | T | W | V | X |

Playfair Cipher Rules and Example

Rules

1.For this course, always combine I/J (do NOT drop Q)

2. When you must select a letter from the I/J box, always choose I.

Example encrypt LARK using playfair cipher with keywork PINK

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P | I/J | N | K | A |
| B | C | D | E | F |
| G | H | L | M | O |
| Q | R | S | T | U |
| V | W | X | Y | Z |

Bigram LA maps to ON

Bigram RK maps to TI

Playfair cipher padding rules

1. split into bigrams ( sleep = SL EX EP)
2. If the last letteris a singleton, pad it with a “Z” to make it a bigram PARTY = PA RT YZ

Examples WIRELESS = WI RE LE SX SZ ACCESS = AC CE SX SZ (Note: 2 Cs not in same bigram

Hill Cipher Example

Let M = “party” = {15,0,17,19,24)

Deals with matrixes

Modulo 26

K = [ 7 -2 ]

[ 4 13]

C(PA) = [ 7 -2 ] [ 15] [ 7\*15+(-2)\*0] [1] = BI

[ 4 13] [ 0 ] = [4\*15 + 13\*0] = [8]

R = 17 T = 19

7\*17 – 2\*19 = [3] = DD

4\*17+13\*19 = [3]

YZ (padded)

7\*24 – 2\*25 = 14

4\*24 + 13\*25 = 5 = OF

Data Encryption Standard S-Box Example

S-boxes Ssub1 and Ssub2 to determine the hexadecimal output for the input BC6sub16.

BC6sub16 = 1011 1100 0110sub2

Input to Ssub1 = higher order six bits = 101111

Input to Ssub2 = lower order six bits = 000110

Take first and last on high order 101111 11 = 3 so third row

Middle four bits select row 0111 = 7 so column 7

Therefor output from Ssub1 is 7base10=7base16

S2 Lower order six bits = 000110 row is 00 =0

Column is 0011 = 3 row 0 column 3

14 base ten is = E base 16

So, result from both S-boxes: BC6 base 16 -> 7E base 16

Number Systems

Decimal, Binary, Octal, and hexadecimal

Two’s complement:

First binary is negative if one. All others are normal

This allows us to go from for example -128-127

To get the complement number switch all 0s and 1s, then add a binary 1

Example 0000 1111 = 15

1111 0001 = -15

to add binary numbers in two’s complement

0+0=0

0+1=1

1+0=1

1+1=0 carry 1

1+1+1=1 carry 1

if a 1 carries to the 5th position i.e. 10010 ignore it!

Overflow in two’s complement

7+5 = 12

cannot put 12 in two’s complement