CIS 3362 Test #2: Modern Symmetric Encryption Schemes (DES, AES), Number Theory Background, Diffie-Hellman Key Exchange

Date: 10/26/2016

Name: ____

1) In DES, which four inputs (of six bits) to S-box $\mathbf{S_6}$ will create the four bit output 1101? (Please express each answer as bit strings of 0s and 1s.)

__________ , __________ , __________ , __________

2) If the input to the E permutation (in the beginning of the Feistel function of DES) is

`3AEF 8301` in hexadecimal, what are the first six hex characters (24 bits) of output?

____

3) In the specification of DES, the key is represented as 64 bits, of which some are parity bits. Label all the bits (including parity bits) as k_1, k_2, ..., k_{64}. If you knew the values of k_1 through k_{16}, but had to perform a brute force search through the other bits of the key, how long, in the worst case, would it take you to find the key, given that you can search through 2^{20} keys in one second? Please express your answer in days, rounded to the nearest day.

____

4) Consider the AES Key Schedule where we have

```
w[20] = 01234567
w[23] = 89abcdef
```

expressed in hex. Calculate w[24], filling in each intermediate step shown below:

RotWord	SubWord	Rcon[i/4]	XOR	FinalResult(w[24])

5) In the AES Mix Columns operation, multiplication between terms must be performed. These multiplications are really in the field GF(2^8). Perform the following two multiplications in that field:

(a) 03 x D3
(b) 04 x C9

Note: Though we didn't explicitly cover how to do (b) in class, you can deduce how to do it by analyzing multiplication by 02, which we did cover in class and applying it to this situation.

(a) 03 x D3 = ________ (b) 04 x C9 = ________

6) What is the prime factorization of 6675696?

____

7) What is φ(10!)?

____

8) Determine the remainder when 47^{267} is divided by 90?

____

9) Consider the Diffie-Hellman key exchange where the public values are p = 29 and g = 10. If Alice chooses a = 8 as her secret key, what value does she send Bob?

____

10) Which presidential candidate claims Trump Tower as a residence? ______________________

Scratch Page - Please clearly mark any work on this page you would like to be graded.