Tutorial 10: Modern Symmetric Ciphers ~ IDEA

1.
   a. Why is the multiplication operation of idea modulo $(2^{16}+1)$ instead of simply 2^{16}?
   b. Why is the addition operation of IDEA modulo 2^{16} instead of $(2^{16}+1)$?

2. Refer to the figure of IDEA in the slides and answer the following:
   a. Reproduce the second round of this diagram, labeling the widths of the data paths shown and explaining the function of the symbols shown in the diagram. Clearly indicate the Multiplication-Addition (MA) structure). What is the purpose of the MA structure in the algorithm?
   b. Given that 2^{128} = 340282366920938463463374607431768211456 and that the IDEA weak keys (that are would not be used are)
      `0000 0000 0x00 0000 0000 000x xxxx x000,`
      Determine the exact keyspace of IDEA. Write down the numerical value in full.
   c. Part of IDEA's key schedule specifies a 25 bit rotation in deriving subkeys. Using this information and the information given in figure 1, write the first four subkeys for the second round into your diagram, given the primary key(in binary notation) below. Specify the required subkeys in hexadecimal notation.

```
10011001100101110011101011101001110000111111100101010100110101101
10011010111010010111011101001010111010001010101011010001101110001
```

3. There are a total of 8×6+4 = 52 subkeys in IDEA. These subkeys are generated as follows: divide the 128 bit key into eight 16-bit subkeys. These 8 keys are the first 8 keys of the algorithm, i.e. $Z_1^{(1)}$, $Z_2^{(1)}$,…,$Z_6^{(1)}$,$Z_1^{(2)}$,$Z_2^{(2)}$. The key is then rotated 25 bits to the left and divided into eight subkeys again. These subkeys form the next eight subkeys for the algorithm. This process is repeated until the end of the algorithm. The seventh rotation produces four subkeys for the final transformation and the remaining four subkeys are discarded.

   The passage above describes the key schedule of IDEA. Determine the number of 25 bit shifts that can take place before a repeated subkey occurs. Suppose that a number other than 25 is to be used for the shift size. What rule(s), to prevent the repetition of subkeys would you make about the selection of this number?

4. Someone proposes that the block size of IDEA be reduced but the key size be kept the same. In what way could this compromise the security of the cipher?

5. Look at the table showing the relationship between ideas encryption and decryption subkeys. Explain the meaning of the symbols in the decryption column and how the decryption subkeys are determined from the encryption subkeys. Why do the subkeys in the decryption stage sometimes produce subkey 2 first, then 3; and in other cases produces subkey 3 first then 2?

6. Do an internet search on the following:
   a. Advanced Encryption Standard (AES).
   b. CAST-128