

Assignment 4 (Topic 5. Symmetric Key Cryptography)

1. What randomness properties that WG cipher has? List them as many as you can. What is the WG transform? Give a WG transform for $n = 7$ and $n = 8$.
2. Using the architecture of Grain 2, let both the LFSR and NLFSR have degree 4. The characteristic polynomial of the LFSR is given by $x^4 + x + 1$ and output is $\{a_i\}$. The feedback of the NLFSR is given by $g(x_0, x_1, x_2, x_3) = x_0 + x_1x_2 + x_2x_3$ and the output is $\{b_i\}$ where the feedback bit is $b_{i+4} = a_i + g(b_i, b_{i+1}, b_{i+2}, b_{i+3})$. The output of the generator is given by

$$s_i = b_i + b_{i+3} + a_i a_{i+2}, i = 0, 1, \dots$$

- (a) List all output sequences of the generator for fixed initial states 0001 and 1010 in the LFSR.
 - (b) What are the periods of those sequences?
3. For DES, explain DES decryption, what conclusion can you derive?
4. If you are approached by a company to design a cipher with low cost. Which type of cipher algorithms that you would like to recommend to them. Justify your answer.

The following questions are optional.

5. Let A^c be the complement of A where A is a binary string (e.g. if $A = 1000100$, then $A^c = 0111011$.)
 - (a) Show that if $Y = DES_k(X)$, then $Y^c = DES_{k^c}(X^c)$.
 - (b) It has been said that a brute-force attack on DES requires searching a key space of 2^{56} keys. Does the result of part (a) change that?
6. For RIJNDAEL,
 - (a) For 128-bit version of RIJNDAE, what is the complexity of placing a brute-force attack on it? Do you know any improvement for this complexity?
 - (b) In the description of RIJNDAEL, the order of performing three basic operators is illustrated in the slides. Explain that why we can change this order to the Word-Operation.