Homework Problems : Stream Ciphers

1. Prove that every *n*-variable Boolean function has a unique Algebraic Normal Form (ANF) representation with *n* variables $\{x_1, x_2, \ldots, x_n\}$.

2. Find out, either theoretically or computationally, the maximum possible non-linearity (based on vectorial Hamming distance) for any 4-variable Boolean function, and construct and/or identify at least one 4-variable Boolean function having the maximum non-linearity.

3. In the output of the RC4 stream cipher (described below), computationally find the probability distribution for the first and second output bytes (z_1 and z_2) with respect to 128-bit (16-byte) keys chosen uniformly at random from $\{0,1\}^{128}$. Try to prove any interesting observation therein.

RC4 Key Scheduling Algorithm (KSA)

```
for i from 0 to 255
    S[i] := i
endfor

j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

RC4 Pseudo-Random Generation Algorithm (PRGA)

```
i := 0
j := 0
while OutputRequired:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```