M1 Int'l, november 21, 2017

TD 2 Cryptography and security

1 Cryptanalysis

(1) Cryptanalyse the following text enciphered by a multiplicative cipher (it is in french):

`RAWFEJBANAREQSSQBDAWKRSKWK`

Most frequent french letters are `ETIANS` (18%,7%,6%6%,6%,6%)

2 Feistel cipher

Show that when inverting the order of the round keys in a Feistel cipher, the same algorithm can be used to decipher and to encipher. Restrict yourselves to a Feistel cipher with two rounds and with $m = n$.

3 Polynomial algebra

(1) Compute the Euclidean division of $x^4 + x + 1$ by $x + 1$. Deduce from the previous question the gcd of the polynomials and the multiplicative inverse of $x + 1$ in $\mathbb{F}_2[x]/x^4 + x + 1$.

(2) Give the multiplication table between elements of the finite field $\mathbb{F}_2[x]/x^2 + x + 1$. Which is this finite field?