Consultation 6

19 November 2020 09:20

$|GF(2^n)| = 2^n$ n-bit strings

$(1\,1\,0\,1\,1) \sim x^4+x^3+x+1$

27

$(11011)\cdot(00101)$ $\quad (x^4+x^3+x+1)\cdot(x^2+1) \mod p(x)$

$27 \quad 5$

$= 155$

irreducible polynomial of degree 5

$a \in GF(2^n)$ order of $GF(2^n)$

a^e in $GF(2^n)$

$\underbrace{f_a(x)\cdot f_a(x)\cdots f_a(x)}_{e}$

$a^{\varphi(n)} \mod n \equiv 1$ iff $\gcd(a,n) = 1$

$a^{p-1} \mod p \equiv 1$

$(a^e)^d \equiv a^{e\cdot d \bmod p-1} \equiv a^1 \bmod p$

$e \quad (e \bmod p-1)$

$a \equiv a \mod p$

$d = e^{-1} \mod (p-1)$

order of multiplication group of $\mathbb{F}_p$ with p prime is $(p-1)$

$(1)^e = 1$

$(-1) = z$

$\text{order}(\mathbb{F}_p) = p-1 \Rightarrow \forall k \in \mathbb{F}_p \; a^{p-1} \equiv 1 \bmod p$

$d = e \mod (p-1)$

$\text{order}(\mathbb{F}_p) = p-1 \Rightarrow \forall a \in \mathbb{F}_p \; a^{p-1} \equiv 1 \mod p$

by Lagrange's theorem order of multiplicative group of $GF(2^4) = 2^4 - 1$

$a \in GF(2^4) \quad a^{2^4-1} \equiv 1 \quad (\text{in } GF(2^4))$

$\gcd(e_A, 2^4 - 1) = 1$

$\exists \, d_A$ s.t. $d_A = e_A^{-1} \mod 2^4 - 1$

Randomized factoring algorithm

$\sqrt{n}$

$A(n)$ ~ chooses a random number $\{2, \ldots, \lfloor \sqrt{n} \rfloor\}$ (assume $n = p \cdot q$)

$\Pr(A(n) \text{ giving a factor}) = \frac{1}{\sqrt{n}} \quad \forall n$

A' ~ has a table T of factors for all numbers $n \leq 100$

$A'(n) =$ if $n \leq 100$ lookup table T and return an answer

otherwise call $A(n)$

$\Pr(A'(n) \text{ giving incorrect answer}) \Rightarrow$ depends on n

for each c (here $c = 1/2$) $\exists \, n_c$ (here $n_c = 100$)

$\forall n > n_c \quad \Pr(\text{correct answer}) \leq \frac{1}{n^c}$

$$P(x \geq k) = \sum_{i=k}^{n} p(i)$$

$$P(x = k) = p(k)$$

$$P(x \geq k) - P(x = k) = \sum_{i=k+1}^{n} p(i)$$

$$= P(x \geq k+1)$$