8

1

a

The polynomial $x^9 + x + 1$ is an irreducible polynomial (over the field $\mathbb{F}_2$), but it is not primitive. Verify this fact.

You do not have to prove that it is irreducible. (HINT: $511 = 7 \times 73$)

✓ **Answer**

$2^9 - 1 = 511$

If root α has order below 511, then the polynomial is not primitive.

$511 = 7 \times 73$

$x^{73} \pmod{x^9 + x + 1}$
$(x^9)^8 x \pmod{x^9 + x + 1}$
$(x + 1)^8 x \pmod{x^9 + x + 1}$
$(x^2 + 1)^4 x \pmod{x^9 + x + 1}$
$(x^4 + 1)^2 x \pmod{x^9 + x + 1}$
$(x^8 + 1) x \pmod{x^9 + x + 1}$
$x^9 + x \pmod{x^9 + x + 1}$
$1 \pmod{x^9 + x + 1}$

Thus $x^9 + x + 1$ is not primitive

b

Verify that the polynomial $x^9 + x^4 + 1$ is indeed primitive.

✓ **Answer**

$2^9 - 1 = 511$

If root α has order below 511, then the polynomial is not primitive.

$511 = 7 \times 73$

$x^{73} \pmod{x^9 + x^4 + 1}$
$(x^9)^8 x \pmod{x^9 + x^4 + 1}$
$(x^4 + 1)^8 x \pmod{x^9 + x^4 + 1}$
$(x^8 + 1)^4 x \pmod{x^9 + x^4 + 1}$

$((x^4+1)x^7+1)^2x \pmod{x^9+x^4+1}$
$(x^{11}+x^7+1)^2x \pmod{x^9+x^4+1}$
$((x^4+1)x^2+x^7+1)^2x \pmod{x^9+x^4+1}$
$(x^7+x^6+x^2+1)^2x \pmod{x^9+x^4+1}$
$(x^{14}+x^{12}+x^4+1)x \pmod{x^9+x^4+1}$
$x^{15}+x^{13}+x^5+x \pmod{x^9+x^4+1}$
$(x^4+1)x^6+(x^4+1)x^4+x^5+x \pmod{x^9+x^4+1}$
$x^{10}+x^8+x^6+x^5+x^4+x \pmod{x^9+x^4+1}$
$(x^4+1)x+x^8+x^6+x^5+x^4+x \pmod{x^9+x^4+1}$
$(x^5+x)+x^8+x^6+x^5+x^4+x \pmod{x^9+x^4+1}$
$x^8+x^6+x^4 \pmod{x^9+x^4+1}$

Thus x^9+x^4+1 is primitive

2

An LFSR of length 9 has connection coefficients $[c_1, c_2, \ldots, c_9] = [0,0,0,1,0,0,0,0,1]$. If the seed is $\sigma = [0,0,0,0,1,1,1,0,0]$, what are the first twenty bits of output? NOTE: The first nine bits are the seed, so start with the tenth bit of output.

For info on LFSR, see http://cacr.uwaterloo.ca/hac/about/chap6.pdf

✓ **Answer**

$[0,0,0,0,1,1,1,0,0] \to 0$
$[0,0,0,0,0,1,1,1,0] \to 0$
$[0,0,0,0,0,0,1,1,1] \to 1$
$[1,0,0,0,0,0,0,1,1] \to 1$
$[1,1,0,0,0,0,0,0,1] \to 1$
$[1,1,1,0,0,0,0,0,0] \to 0$
$[0,1,1,1,0,0,0,0,0] \to 1$
$[1,0,1,1,1,0,0,0,0] \to 1$
$[1,1,0,1,1,1,0,0,0] \to 1$
$[1,1,1,0,1,1,1,0,0] \to 0$
$[0,1,1,1,0,1,1,1,0] \to 1$
$[1,0,1,1,1,0,1,1,1] \to 0$
$[0,1,0,1,1,1,0,1,1] \to 0$
$[0,0,1,0,1,1,1,0,1] \to 1$
$[1,0,0,1,0,1,1,1,0] \to 1$
$[1,1,0,0,1,0,1,1,1] \to 1$
$[1,1,1,0,0,1,0,1,1] \to 1$
$[1,1,1,1,0,0,1,0,1] \to 0$
$[0,1,1,1,1,0,0,1,0] \to 1$

$[1,0,1,1,1,1,0,0,1] \to 0$
$[0,1,0,1,1,1,1,0,0] \to 1$

3

Assume that the entropy per letter of English words is 1.25 bits per letter. Paul has a fourteen letter secret key which is known to have been taken from English text.

a

Approximately what is the entropy of Paul's secret key if he only uses small letters?

Example: `axiomaticideas`

✓ **Answer**
$1.25 \times 14 = 17.5 \text{ bits}$

b

Approximately what is the entropy of Paul's secret key if he only uses a random mix of small and capital letters?

Example: `axIOmAtiCiDeas`

✓ **Answer**
$1.25 \text{ bits} + 1 \text{ bits}$
$2.25 \times 14 = 31.5 \text{ bits}$

c

If in addition to using random capitals as in the previous part, he then inserts one of sixteen possible special characters between two of the letters of his key, what is the approximate entropy of his key?

Example: `axIOmA@tiCiDeas`

✓ **Answer**
31.5 bits before the adding of the symbol
Position of the symbol: $\log_2 15$
Choice of symbol: $\log_2 16$

$H = 33.5 + \log_2 15 \approx 37.41 \text{ bits}$