Mid-Term Review

Camryn Truban

March 9th, 2020

Mssion 4 Problem 4: Find the last two digits of $4^{3^{210}}$

Given that we are looking for the last two digits we will me using (mod100)
$4^{3^{210}}$(mod100)
3^{210}(modφ100)
φ100=40
3^{210}(mod40) = 3
3^1(mod40)=9 4^1(mod100)=4
$3^2(mod40) = 9$ 4^2(mod100)=16
$3^4(mod40) = 27$ 4^4(mod100)=54
$3^8(mod40) = 1$ 4^8(mod100)=36
$3^{16}(mod40) = 1$
$3^{32}(mod40) = 1$
$3^{64}(mod40) = 1$
$3^{128}(mod40) = 1$
210 = 128+64+16+2 (9*1*1*1)mod40=9
4^9(mod100)=4*36(mod100)=44
$4^{3^{210}}$(mod100)=44

Mssion 4 Problem 3: Write down all of the 8 elements of field of 8 using the irreducible polynomial $x^3 + x + 1$
Multiply each element by $x^2 + 1$

*	$x^2 + 1$
0	0
1	$x^2 + 1$
x	x
x+1	$x^2 + x + 1$
x^2	x
$x^2 + 1$	$x^2 + x + 1$
$x^2 + x$	x+1
$x^2 + x + 1$	$x^2 + x$

Missiong 5 Problem 4: Use Euclid's algorithm to find the inverse of f(x) = x^2 inthe field F8 with irreducible polynomial x^3+x+1
gcd(x^3+x+1, x^2)
$x^3+x+1 = x^2(x)+(x+1)$
x^2=(x+1)(x+1)+1
1=$x^2-(x+1)(x+1)$
x+1=(x^3+x+1)-x(x^2)
1=$x^2-(x+1)((x^3+x+1)+x(x^2))$
$(x^2+x)(x^2)$
1=$(x^2+x+1)(x^2)(mod x^3+x+1)$
$(x^2)^{-1} = x^2+x+1$

DES
The worksheet provided helps us encrypt 12-bit
-It is usually more than 12 bits though
So how would we encrypt 1000-bits?
-Encrypt 12-bits at a time.
Encrypting Plaintext longer than blocksize
First Idea: Break plaintext into chunks of size of a block, encrypt each blod seperatly(*Mode of Operation*)