Tristan Erney
October 19th, 2021
Intro to Cryptology
Hands On Exercise 7 – Finite Fields

#1

M = $x^8 + x^4 + x^3 + x + 1$ = 1 0 0 0 1 1 0 1 1

								1	1	0	0	0	1	0	0
							x	1	0	1	1	0	0	0	1
								1	1	0	0	0	1	0	0
				1	1	0	0	0	1	0	0				
			1	1	0	0	0	1	0	0					
	1	1	0	0	0	1	0	0							
	1	1	1	0	1	1	0	0	0	0	0	0	1	0	0

→ $x^{14} + x^{13} + x^{12} + x^{10} + x^9 + x^2$

	1	1	1	0	1	1	0	0	0	0	0	0	1	0	0	
xor	1	0	0	0	1	1	0	1	1							
	0	1	1	0	0	0	0	1	1	0	0	0	1	0	0	
		1	0	0	0	1	1	0	1	1						
		0	1	0	0	1	1	1	0	1	0	0	1	0	0	
			1	0	0	0	1	1	0	1	1					
			0	0	0	1	0	0	0	0	1	0	1	0	0	
						1	0	0	0	1	1	0	1	1		
						0	0	0	0	1	0	0	0	1	0	→ $x^5 + x$

#2

97 * s + 60 * t = gcd(97, 60) = 1 (mod 97)

97 = (1)60 + 37	37 = 97 – (1)60
60 = (1)37 + 23	23 = 60 – (1)37
37 = (1)23 + 14	14 = 37 – (1)23
23 = (1)14 + 9	9 = 23 – (1)14
14 = (1)9 + 5	5 = 14 – (1)9
9 = (1)5 + 4	4 = 9 – (1)5
5 = (1)4 + 1	1 = 5 – (1)4
4 = (4)1 + 0	

1 =	(1)5 – (1)4	=	(1)5 – (1)(9 – (1)5)
	(2)5 – (1)9	=	(2)(14 – (1)9) – (1)9
	(2)14 – (3)9	=	(2)14 – (3)(23 – (1)14)
	(5)14 – (3)23	=	(5)(37 – (1)23) – (3)23
	(5)37 – (8)23	=	(5)37 – (8)(60 – (1)37)
	(13)37 – (8)60	=	(13)(97 – (1)60) – (8)60
	(13)97 – (21)60		

1 = 97 * 13 + 60 * -21

60^{-1} = -21 = 76 (mod 97)

#3

$$\begin{array}{rl}
 & \underline{x^4 + x^3 + x^2 + x + 1} \\
x^4 + x^3 + 1 & \big) x^8 + x^4 + x^3 + x + 1 \\
- & \underline{x^8 + x^7 + x^3} \\
 & \quad x^7 + x^3 + x + 1 \\
 & \quad \underline{x^7 + x^6 + x^3} \\
 & \qquad x^6 + x + 1 \\
 & \qquad \underline{x^6 + x^5 + x^2} \\
 & \qquad\quad x^5 + x^2 + x + 1 \\
 & \qquad\quad \underline{x^5 + x^4 + x} \\
 & \qquad\qquad x^4 + x^2 + 1 \\
 & \qquad\qquad \underline{x^4 + x^3 + 1} \\
 & \qquad\qquad\quad x^3 + x^2
\end{array}$$

$$\begin{array}{rl}
 & \underline{x \qquad\qquad} \\
x^3 + x^2 & \big) x^4 + x^3 + 1 \\
 & \underline{x^4 + x^3 \qquad} \\
 & \qquad\qquad 1
\end{array}$$

A = $(x^4 + x^3 + x^2 + x + 1) * b + (x^3 + x^2)$

B = $(x) * (x^3 + x^2) + 1$

1 = $B – (x) * (x^3 + x^2)$

$B – (x) * \{ A – (x^4 + x^3 + x^2 + x + 1) * B \}$

$B – (x) * A + (x^4 + x^3 + x^2 + x + 1)(x) * B$

$-(x) * A + (x^5 + x^4 + x^{3\,+} x^2 + x + 1) * B$

B^{-1} = $x^5 + x^4 + x^3 + x^2 + x + 1$