Midterm

Colin Quinn

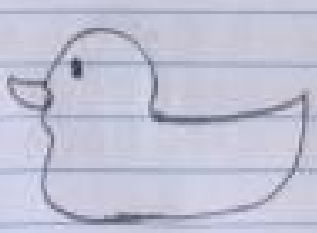
1. a. $3 \cdot 1/5 \bmod 26$
$3 \cdot (5x) \equiv 1 \bmod 26$
$3x\ 21 \equiv 1 \bmod 26$
$3 \cdot 1 = (3)$

b. $y = (21x + 15) \bmod 26$ where $x = 25$
$A = 21,\ A' = 5$
$B = 15,\ B' = 15$ ∴ Z decrypts to Y

2. Encryption: $y_i = e_{s_i}(x_i) \equiv x_i + s_i \bmod 2$
Decryption: $x_i = d_{s_i}(y_i) \equiv y_i + s_i \bmod 2$
- Keys are usually generated in lengths of 128 bits
- Known plaintext attacks. Find the most common values and compare them.

3. I am honestly not sure how to do this. However using the S-box and finding 22 in the values of the table gives us 94 as the answer. (=94)

Instead of the math, please enjoy the rubber ducky I talked this problem through with.



4 ECB lacks integrity because of its highly deterministic nature, and is susceptible to substitution attacks.

CBC: Encryption $y_0 = e_k(x_0 \oplus IV)$

$y_i = e_k(x_i \oplus y_{i-1}),\ i \geq 2$

Decryption: $x_1 = e_k^{-1}(y_1) \oplus IV$

$x_i = e_k^{-1}(y_i) \oplus y_{i-1},\ i \geq 2$

We can now select a different IV for each encryption, this IV value makes the same plaintext look completely different and does not have to be secret.

5. A) 128 bits

B)
$$\begin{bmatrix} 8A \\ 01 \\ 01 \\ 01 \end{bmatrix} \times \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} = \begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix}$$

$01 = 1$
$02 = x$
$03 = x+1$

$C_0 = 02 \cdot 8A \oplus 03 \cdot 01 \oplus 01 \cdot 01 \oplus 01 \cdot 01$

$02 \cdot 8A = x(x^7 + x^3 + x)$
$= x^8 + x^4 + x$ where $x^8 = x^4 + x^3 + x + 1$
$= (x^4 + x^3 + x + 1) + x^4 + x$
$= x^4 + 1$
$= 0001\ 0001$

$03 \cdot 01 = x + 1(1)$
$= x + 1$
$= 0000\ 0011$

$01 \cdot 01 = 0000\ 0001$

$$\begin{array}{r} 0001\ 0001 \\ 0000\ 0011 \\ 0000\ 0001 \\ \oplus\ 0000\ 0001 \\ \hline C_0 = \ 0001\ 0010 \end{array} = (12)$$

$C_1 = 01 \cdot 8A \oplus 02 \cdot 01 \oplus 03 \cdot 01 \oplus 01 \cdot 01$

$01 \cdot 8A = 1000\ 1010$
$02 \cdot 01 = 0000\ 0010$

$$\begin{array}{r} 1000\ 1010 \\ 0000\ 0010 \\ 0000\ 0011 \\ \oplus\ 0000\ 0001 \\ \hline C_1 = \ 1000\ 1010 \end{array} = (8A)$$

$C_2 = 8A \cdot 01 \oplus 01 \cdot 01 \oplus 01 \cdot 02 \oplus 01 \cdot 03$

$8A \cdot 01 = 1000\ 1010$
$01 \cdot 01 = 0000\ 0001$
$01 \cdot 02 = 0000\ 0010$
$01 \cdot 03 = 0000\ 0011$

$1000\ 1010$
$0000\ 0001$
$0000\ 0010$
$\oplus\ 0000\ 0011$
$C_2 = 1000\ 1010 = 8A$

$C_3 = 8A \cdot 03 \oplus 01 \cdot 01 \oplus 01 \cdot 01 \oplus 01 \cdot 02$

$8A \cdot 03 = x+1\,(x^7 + x^3 + x)$
$= x^8 + x^4 + x^2 + x^7 + x^3 + x \rightarrow x^7 + x^3 + x^4 + x^3 + x^2 + x$

where $x^8 = x^4 + x^3 + x + 1 \rightarrow (x^4 + x^3 + x + 1) + x^7 + x^4 + x^3 + x^2 + x$
$= x^7 + x^2 + 1 = 1000\ 0101$

$01 \cdot 01 = 0000\ 0001$
$01 \cdot 02 = 0000\ 0010$

$1000\ 0101$
$0000\ 0001$
$0000\ 0001$
$\oplus\ 0000\ 0010$
$C_3 = 1000\ 0111 = 87$

$$\begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} 12 \\ 8A \\ 8A \\ 87 \end{bmatrix}$$

6. gcd(42, 191)

q_{i+1}	r_i	s_i	t_i
42	191	0	1
191	42	1	0
42	23	-4	1
23	19	5	-1
19	4	-9	2
4	3	41	-9
3	1	-50	11

08 $s = -50$, $t = 11$

7. A) 5 is not divisible by 11, therefore.

$5^{11-1} \equiv 1 \bmod 11$

$5^{10} \equiv 1 \bmod 11$

$9765625 \equiv 1 \bmod 11$

$= (9765625/11) \equiv 1 \bmod 11$

$= 887784 + 1$ so likely is prime.

B) $\phi(5) = 4$

This is because 5 is prime, so $\phi(n) = n-1$.