CIS3362 12/1/2021

1) X = # zeroes

$100 - X$ = # ones

$$\frac{X(X-1) + (100-X)(99-X)}{100 \times 99} = \frac{19}{33}$$

$$X^2 - X + 9900 - 199X + X^2 = \frac{19 \times 100 \times \cancel{99}^{3}}{\cancel{33}}$$

$$2X^2 - 200X + 9900 = 5700$$

$$2X^2 - 200X + 4200 = 0$$

$$X^2 - 100X + 2100 = 0$$

$$(X - 30)(X - 70)$$

$$X = 30, 70$$

Answer = 40

2) $f(x) = (28x + 33) \bmod 65$

$$x = (28y + 33) \bmod 65$$

$$(x - 33) \equiv 28y \bmod 65$$

$65 = 2 \times 28 + 9$

$28 = 3 \times 9 + 1$

$28 - 3 \times 9 = 1$

$28 - 3(65 - 2 \times 28) = 1$

$28 - 3 \times 65 + 6 \times 28 = 1$

$7 \times 28 - 3 \times 65 = 1$

$$7(x - 33) \equiv y \bmod 65$$

$$y = (7x - 231) \bmod 65$$

$$\boxed{y = 7x + 29 \bmod 65}$$

3)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1	0	0	1	1	1	1	0	1	1	1	1	0	0	1

Output: 0010 1101 1110 1011

2 D E B

4) 03 × B6

01 × B6 = 1011 0110

02 × B6 =

$$\begin{array}{r} 1011\ 0110 \\ \times\ 0110\ 110 \\ \hline 1\ 1\ 0\ 1\ 1 \\ \hline 1100\ 0001 \end{array}$$

$$\begin{array}{r} 1011\ 0110 \\ 1100\ 0001 \\ \hline 0111\ 0111 \end{array}$$

77

5) Want terms such that

$g^1, g^2, \ldots \not\equiv 1 \bmod p$

but $g^{\frac{p-1}{2}} \equiv 1 \bmod p$ (period to be half of p-1)

$g^x \Rightarrow$ all terms can be written like this

$(g^x)^{\frac{p-1}{2}} = g^{(p-1)y}$ for some int y.

Once we cancel the 2 in x, it can't share any further factors with $p-1$. $\Rightarrow \gcd(x, p-1) = 2$

how many even numbers $\gcd(x, \frac{p-1}{2}) = 1$

$\phi(\frac{p-1}{2})$

7) If both use the same n, they know the other person's p and q and knowing their other person's e can calculate the other person's d. Once they know this, they can sign as the other person!

8) 2 people for
2 people Dec

Sample Space $= 12^4$

$6 = \binom{4}{2}$

A, A, D, D
A D A D
A D D A
D A A D
D A D A
D D A A

} 6 ways fixed for 2 months

$\binom{12}{2}$ choose 2 month out of 12

$$\frac{12 \times 11}{2} = 66$$

$$P = \frac{\cancel{6} \times \cancel{66}^{\cancel{33}^{11}}}{\cancel{12} \times \cancel{12} \times 12^2} = \boxed{\frac{11}{576}}$$

$\cancel{12}$ 4

144
4
576