1) $y = 100 - x$

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

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

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

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

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

$$(x - 30)(x - 70) = 0$$

$x = 30$ or $x = 70$

$|70 - 30| = \boxed{40}$

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

$x = 28y + 33 \mod 65$

$7(28y) = 7(x - 33) \mod 65$

$y \equiv (7x - 231) \mod 65$

$\boxed{f^{-1}(x) = 7x + 29 \mod 65}$

$28^{-1} \mod 65$

$65 = 2 \times 28 + 9$

$28 = 3 \times 9 + 1$

$28 - 3 \times 9 = 1$

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

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

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

$\begin{array}{r} 65 \\ 4 \\ \hline 260 \end{array}$ $\quad$ $\begin{array}{r} 33 \\ 7 \\ \hline 231 \end{array}$

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

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

2DEB

4) 03 × B6

B6 = 1011 0110

02 × B6 = 1 0110 1100
⊕ 1011

02 × B6 = 0111 0111
01 × B6 ⊕ 1011 0110

03 × B6 = 1100 0001

C1

5) Generator 3 mod 7

3, 2, 6, 4, 5, 1

2, 4, 1, 2, 4, 1

g^x is a half-gen iff $\gcd(x, p-1) = 2$

$\gcd\left(\frac{x}{2}, \frac{p-1}{2}\right) = 1$

values of $\frac{x}{2}$ share a gcd of 1 w/ $\frac{p-1}{2}$ is

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

7) $\lambda = \frac{7-13}{35-24} = \frac{-6}{11} = (-6) * (11^{-1} \bmod 47)$

Pt (24, 13) P
Pt (35, 7) Q
$E_{47}(10, 17)$.

$47 = 4 \times 11 + 3$
$11 = 3 \times 3 + 2$
$3 = 1 \times 2 + 1$
$3 - 1 \times 2 = 1$
$3 - (11 - 3 \times 3) = 1$
$4 \times 3 - 11 = 1$
$4(47 - 4 \times 11) - 11 = 1$
$4 \times 47 - 16 \times 11 - 1 \times 11 = 1$
$4 \times 47 - 17 \times 11 = 1$
$11^{-1} \equiv -17 \pmod{47}$

$R = (5, 45)$

$\lambda = (-6)(-17) \bmod 47$
$= 102 \bmod 47$
$= 8$

$x_R = (\lambda^2 - x_P - x_Q) \bmod 47$
$= 64 - 24 - 35 \bmod 47$
$= \boxed{5}$

$y_R = (\lambda(x_P - x_R) - y_P) \bmod 47$
$= 8(24 - 5) - 13 \bmod 47$
$= 8 \times 19 - 13$
$= 152 - 13$
$= 139$
$= \boxed{45}$

$139 - 94 = 45$

Side note:

P 1. (7, 12)
2P 2. (3, 10)
3P 3. ...
⋮

20. Origin
21. (7, 12)
⋮

$(18, 3) + (12, 11)$
$\Downarrow \quad \downarrow$
$13^{th} + 15^{th} = 28^{th}$

$28 \bmod 20$
$\Rightarrow 8^{th}$ #

8) Sample Space $= 12^4$

Jan Jan Mar Mar] How many Strings have 2 + 2

$\binom{12}{2}$: Choose 2 months out of 12

$\times \binom{4}{2}$: Choose 2 slots out of 4 for Jan

$$\frac{\frac{12\times 11}{2} \times \cancel{6}\ 3}{12^4} = \frac{\cancel{12} \times 11 \times \cancel{3}}{\cancel{12}\times\cancel{12}\times 12\times 12} = \boxed{\frac{11}{576}}$$

$\begin{array}{r} 144 \\ 4 \\ \hline 576 \end{array}$