Exercise 1

(1) $5^2 \equiv 25 \mod 1979$

$5^4 \equiv 625 \cdots$

$5^8 \equiv 762$

$5^{17} \equiv 27$

$5^{35} \equiv 1666$

$5^{71} \equiv 1032$

$5^{143} \equiv \boxed{1610} \mod 1979$

$2^2 \equiv 4 \mod 1979$

$2^4 \equiv 16 \mod 1979$

$2^8 \equiv 256 \cdots$

$2^{17} \equiv 458$

$2^{35} \equiv 1959$

$2^{71} \equiv 800$

$2^{143} \equiv \boxed{1566} \mod 1979$

(2) $G = \mathbb{F}_{13}^{\times}$:

g	1	2
ord(g)	1	12

$G = \mathbb{F}_{31}^{\times}$:

g	1	2	3
ord(g)	1	5	30

$G = \mathbb{F}_{47}^{\times}$:

g	1	2	3	4	5
ord(g)	1	23	23	23	46

$G = \mathbb{F}_{41}^{\times}$:

g	1	2	3	4	5	6
ord(g)	1	20	8	10	20	40

(3) $G = \mathbb{Z}[i]/3$:

g	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
ord(g)	1	2	4	8	8	4	8	8

$\boxed{1+i}$ is a primitive root in $\mathbb{Z}[i]/3$.

(4) $\boxed{x}$ is a primitive root in $\mathbb{F}_2[x]/(x^4+x+1)$ because 15 is the smallest k where $x^k \mod x^4+x+1 = 1 \pmod 2$.

Exercise 3

~~(1) I will choose a = b = 2. Now,~~

(1) $X \equiv g^a \bmod p \Rightarrow a \equiv \log_g(X) \equiv \log_5(38) \bmod 47.$

$\Rightarrow a \equiv 17$ because $5^{17} \equiv 38 \bmod 47.$

Now, $Z = Y^a = 3^{17} \equiv 2 \bmod 47 \Rightarrow 2$ is the key

$\Rightarrow$ shift everything back 2 spots $\Rightarrow$ $\boxed{\text{CONGRATULATIONS}}$

(2) $KO = 83 \Rightarrow 83^7 \equiv \boxed{534} \bmod 1517$

$NA = 72 \Rightarrow 72^7 \equiv \boxed{1130} \bmod 1517$

(3) $\varphi(1517) = \varphi(37)\varphi(41) = 36 \times 40 = 1440$

Find mult inverse of 11:

r: 1440 11 10 1

q: 130; 1 10

mult. inv.

$\Rightarrow 11 \times 131 \equiv 1 \bmod 1440$

$$d = 131 \Rightarrow \left\{ \begin{array}{l} 1373^{131} \equiv 62 \bmod 1517 \\ 1149^{131} \equiv 42 \bmod 1517 \\ 108^{131} \equiv 53 \bmod 1517 \end{array} \right\} \begin{array}{c} 6\ 2\ 4\ 2\ 5\ 3 \\ \boxed{\text{M A H A L O}} \end{array}$$

(4) (a) AHA
242 $\Rightarrow 242^5 \equiv \boxed{39398} \bmod 39597$

~~(b) MOANA 63272 $\Rightarrow$ $63272^7 \equiv 144 \bmod 208$~~

(b) $\varphi(208) = \varphi(11)\varphi(19) = 180$.

r: 180 7 5 2 1

q: 25; 1 2 2 $\Rightarrow 7 \times 77 \equiv -1 \bmod 180$

77/3 3/2 2/1

2/3 1/2

$\Rightarrow 7 \times 103 \equiv 1 \bmod 180$

d

digital sig: MO AN A
63 27 2 $\Rightarrow$

$$\left.\begin{cases} 63^{103} \equiv 15 \\ 27^{103} \equiv 131 \\ 2^{103} \equiv 128 \end{cases}\right\} \bmod 208$$

add it to message:

$$\left.\begin{aligned} 15^5 &\equiv 7032 \\ 131^5 &\equiv 13760 \\ 128^5 &\equiv 35573 \end{aligned}\right\} \bmod 39597$$

new message: 39398, $\overbrace{7032,\ 13760,\ 35573}^{\text{signature}}$

(c) $39597 + 4$ is a perfect square and equals 199^2.

Therefore, $39597 = 199^2 - 2^2 = (199-2)(199+2)$
$= \boxed{197 \times 201}$