3

2.4

Compute the following discrete logarithms.

a

$\log_2(13)$ for the prime 23, i.e. $p = 23$, $g = 2$, and you must solve the congruence $2^x \equiv 13 \pmod{23}$.

✓ **Answer**

$2^7 \equiv 13 \pmod{23}$

$x = 7$

b

$\log_{10}(22)$ for the prime $p = 47$.

✓ **Answer**

$10^{11} \equiv 22 \pmod{47}$

$x = 11$

c

$\log_{627}(608)$ for the prime $p = 941$.

✓ **Answer**

$627^{18} \equiv 608 \pmod{941}$

$x = 18$

Source

Wrote and used this simple python script:

```
def find_log(b, v, p):
        c = 1
        prod = b
        while prod ≠ v:
                c += 1
```

```
                prod = (prod*b) % p
        return c
```

2.6

Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for a Diffie–Hellman key exchange. Alice sends Bob the value $A = 974$. Bob asks your assistance, so you tell him to use the secret exponent $b = 871$. What value B should Bob send to Alice, and what is their secret shared value? Can you figure out Alice's secret exponent?

✓ **Answer**

$B = g^b \mod p$

$= 805$

$s = A^b \mod p$

$= 397$

Using the same python code listed above, we may brute force for a of

$a = 587$

For larger numbers, this should be extremely hard, however