2

1.43

Consider the affine cipher with key $k = (k_1, k_2)$, whose encryption and decryption functions are given by

- $e_k(m) = k_1 \cdot m + k_2 \pmod{p}$
- $d_k(c) = k_1' \cdot (c - k_2) \pmod{p}$ where $k_1' = k_1^{-1} \pmod{p}$.

a

Let $p = 541$ and let the key be $(34, 71)$. Encrypt the message $m = 204$. Decrypt the ciphertext $c = 431$.

✓ **Answer**

$e_k(204) = 34 \cdot 204 + 71 \pmod{541}$
$\equiv 515$

$k_1' = 366$

$d_k(431) = 366 \cdot (431 - 71) \pmod{541}$
$\equiv 297$

b

Assuming that p is public knowledge, explain why the affine cipher is vulnerable to a chosen plaintext attack. How many plaintext/ciphertext pairs are likely to be needed in order to recover the private key?

✓ **Answer**

Two pairs are enough to determine the original private key pair.

With two pairs, we can easily solve a linear system for both of the private key values.

c

Alice and Bob decide to use the prime $p = 601$ for their affine cipher. The value of p is public knowledge, and Eve intercepts the ciphertexts $c_1 = 324$ and $c_2 = 381$ and also manages to find out that the corresponding plaintexts are $m_1 = 387$ and $m_2 = 491$. Determine the private key and then use it to encrypt the message $m_3 = 173$.

✓ **Answer**

$387 \rightarrow 324$
$491 \rightarrow 381$
$p = 601$

$387k_1 + k_2 \equiv 324 \pmod{601}$
$491k_1 + k_2 \equiv 381 \pmod{601}$
$104k_1 \equiv 57 \pmod{601}$
$104^{-1} = 549$
$k_1 \equiv 549(57) \pmod{601}$
$k_1 \equiv 41 \pmod{601}$
$k_2 \equiv 83 \pmod{601}$
$k = (41, 83)$

$e_k(173) = 173 \cdot 41 + 83 \pmod{601}$
$e_k(173) \equiv 565 \pmod{601}$
$173 \rightarrow 565$

d

Suppose now that p is not public knowledge. Is the affine cipher still vulnerable to a known plaintext attack? If so, how many plaintext/ciphertext pairs are likely to be needed in order to recover the private key?

✓ **Answer**

No, it will no longer be nearly as vulnerable to such an attack.

It would take significantly more time to derive p given known pairs. The only information we have about p is that it is larger than any message sent, which may help determine a possible fitting prime based on the size of the encrypted message.

This method would take significantly more messages to get a possibly close p, but would still require brute force to determine and test possible ps before even determining k.

1.47

Alice and Bob choose a key space $\mathcal{K}$ containing 2^{56} keys. Eve builds a special purpose computer that can check 10^{10} keys per second.

a

How many days does it take Eve to check half the keys in $\mathcal{K}$?

✓ **Answer**

$\frac{2^{55}}{10^{10} \cdot 60 \cdot 60 \cdot 24} = 41.69999654972681$

≈ 42 days

b

Alice and Bob replace their key space with a larger set containing 2^B keys. How large should Alice and Bob choose B in order to force Eve's computer to spend 100 years checking half the keys?

✓ **Answer**

$100 \cdot 365.25 \cdot 24 \cdot 60 \cdot 60 \cdot 10^{10} = 2^{64.77462129339004}$

$B \geq 65.77$

$B = 66$