

Midterm

Solutions

Problem I

1. If K_1 and K_2 are chosen randomly then K is random. Therefore the cipher C is secure.
2. If $K_2 = r(K_1)$ then K is symmetric. Subsequently the one-time pad is used twice and the cipher is *not* secure.
3. If $K_2 = K_1$ then K is composed of zeros only. The cipher can hardly be more insecure since the ciphertext is exactly the plaintext!.

Problem II

1. According to the RSA algorithm,

$$\begin{aligned} C &\equiv M^e \pmod{n} \\ &\equiv 26^{13} \pmod{77} \\ &\equiv 75 \end{aligned}$$

2. According to the RSA algorithm,

$$\begin{aligned} M' &\equiv C^d \pmod{n} \\ &\equiv 75^{37} \pmod{77} \\ &\equiv 26 \end{aligned}$$

As expected $M' = M$.

3. We have $n = 7 \times 11$ therefore $p = 7$ and $q = 11$. Hence:

$$\phi = (p - 1)(q - 1) = 70$$

To recover d , one needs to compute the modular inverse of $e = 13$ modulo $\phi = 70$. Let us start with the computation of the greater common divisor of 70 and 13.

$$\begin{aligned} 70 &= 5 \times 13 + 5 \\ 13 &= 2 \times 5 + 3 \\ 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \end{aligned}$$

Therefore:

$$\begin{aligned} 1 &= 3 - 1 \times 2 \\ &= 3 - (5 - 1 \times 3) \\ &= 2 \times 3 - 5 \\ &= 2 \times (13 - 2 \times 5) - 5 \\ &= 2 \times 13 - 5 \times 5 \\ &= 2 \times 13 - 5 \times (70 - 5 \times 13) \\ &= 27 \times 13 - 5 \times 70 \end{aligned}$$

The identity $27 \times 13 - 5 \times 70 = 1$ leads to

$$27 \times 13 \equiv 1 \pmod{70}$$

Therefore 27 is the modular inverse of 13 modulo 70. This is the number d which is sought.