M/CS 478 Assignment 2

Isaac Boaz

February 12, 2024

1.32

For each of the following primes p and numbers a, compute $a^{-1} \bmod p$ in two ways: (i) Extended Eucldiean Algorithm and (ii) Fast Power Algorithm and Fermat's Little Theorem.

a) $p = 47$ and $a = 11$

(i) Using the Extended Euclidean Algorithm

$$\begin{aligned} 47 &= 4(11) + 3 && \rightarrow 3 = 47 - 4(11) \\ 11 &= 3(3) + 2 && \rightarrow 2 = 11 - 3(3) \\ 3 &= 1(2) + 1 && \rightarrow 1 = 3 - 1(2) \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 1(2) \\ &= 3 - (11 - 3(3)) \\ &= 4(3) - 11 \\ \\ &= 4(47 - 4(11)) - 11 \\ &= 4(47) - 16(11) - 11 \\ &= \cancel{4(47)} - 17(11) \\ &\implies -17 \equiv 30 \pmod{47} \end{aligned}$$

(ii) Using the Fast Power Algorithm and Fermat's Little Theorem

$$\begin{aligned} 11^{47-2} &\equiv 11^{45} \pmod{47} \\ &\equiv 11^{32+8+4+1} \pmod{47} \\ &\equiv 11^{32} \cdot 11^{8} \cdot 11^{4} \cdot 11 \pmod{47} \\ &\equiv 9 \cdot 12 \cdot 24 \cdot 11 \pmod{47} \\ &\equiv 30 \pmod{47} \end{aligned}$$

b) $p = 587$ and $a = 345$

(i) Using the Extended Euclidean Algorithm

$$\begin{aligned}
587 &= 1(345) + 242 & &\rightarrow 242 = 587 - 345\\
345 &= 1(242) + 103 & &\rightarrow 103 = 345 - 242\\
242 &= 2(103) + 36 & &\rightarrow 36 = 242 - 2(103)\\
103 &= 2(36) + 31 & &\rightarrow 31 = 103 - 2(36)\\
36 &= 1(31) + 5 & &\rightarrow 5 = 36 - 31\\
31 &= 6(5) + 1 & &\rightarrow 1 = 31 - 6(5)\\
5 &= 5(1) + 0 & &
\end{aligned}$$

$$\begin{aligned}
1 &= 31 - 6(5)\\
&= 31 - 6(36 - 31)\\
&= 7(31) - 6(36)\\
&= 7(103 - 2(36)) - 6(36)\\
&= 7(103) - 20(36)\\
&= 7(103) - 20(242 - 2(103))\\
&= 47(103) - 20(242)\\
&= 47(345 - 242) - 20(242)\\
&= 47(345) - 67(242)\\
&= 47(345) - 67(587 - 345)\\
&= 114(345) - \cancel{67(587)}\\
&\equiv 114 \pmod{587}
\end{aligned}$$

(ii) Using the Fast Power Algorithm and Fermat's Little Theorem

$$\begin{aligned}
345^{587-2} &\equiv 345^{585} \pmod{587}\\
&\equiv 345^{512+64+8+1} \pmod{587}\\
&\equiv 345^{512} \cdot 345^{64} \cdot 345^{8} \cdot 345 \pmod{587}\\
&\equiv 419 \cdot 529 \cdot 177 \cdot 345 \pmod{587}\\
&\equiv 114 \pmod{587}
\end{aligned}$$

1.34

Recall that g is a primitie root mod p if the powers of g generate all nonzero elements of $\mathbb{F}_p$.

(a) For which of the following primes is 2 a primitive root $\pmod{p}$?

(i) 2 is not a primitive root mod 7 because $2^3 \equiv 1 \pmod{7}$.

(ii) 2 is a primitive root mod 13.

(iii) 2 is a primitive root mod 19.

(iv) 2 is not a primitive root mod 23 because $2^{11} \equiv 1 \pmod{23}$.

(b) For which of the following primes is 3 a primitive root $\pmod{p}$?

(i) 3 is a primitive root mod 5.

(ii) 3 is a primitive root mod 7.

(iii) 3 is not a primitive root mod 11 because $3^5 \equiv 1 \pmod{11}$.

(iv) 3 is a primitive root mod 17.

(e) Primitive roots of 229: [6, 7, 10, 23, 24, 28, 29, 31, 35, 38, 39, 40, 41, 47, 50, 59, 63, 65, 66, 67, 69, 72, 73, 74, 77, 79, 87, 90, 92, 96, 98, 102, 105, 110, 112, 113, 116, 117, 119, 124, 127, 131, 133, 137, 139, 142, 150, 152, 155, 156, 157, 160, 162, 163, 164, 166, 170, 179, 182, 188, 189, 190, 191, 194, 198, 200, 201, 205, 206, 219, 222, 223]. $72 = \Phi(228)$.

(f) 3 5 11 13 19 29 37 53 59 61 67 83

1.47

$$10,000,000,000,000 = 10^{10}$$

(a) Solving for how many days to check half the keys in $\mathbb{K}$:

$$60 \cdot 60 \cdot 24 \cdot 10^{10} = 8.64 \cdot 10^{14} \text{ / day}$$
$$\frac{2^{55}}{8.64 \cdot 10^{14}} \approx 41.7 \text{ days}$$

1.48

Since XOR is a symmetrical operation where you only need to know two of the three values (Source, Key, or Cipher), knowing two of the three gives you the third. As such, the key used to encrypted the message

1001010001010111 given the plaintext
0010010000101100 is just the XOR of the two, ie.
1011000001111011.

2.4

(a) $2^7 \equiv 13 \pmod{23}$

(b) $10^{11} \equiv 22 \pmod{47}$

2.9

If Eve was able to compute $g^{uv} \pmod{p}$ then since Bob and Alice's public keys are essentially $g^u \pmod{p}$ and $g^v \pmod{p}$, respectively, then Eve would be able to compute the shared secret key $g^{uv} \pmod{p}$.