Diskrete Mathematik - Übungen SW11

David Jäggli

10. Mai 2023

Inhaltsverzeichnis

1 Einführung in die Zahlentheorie III

I.)
Weis nicht ob das genügt, aber ist der output 00, ist automatisch der input 1 $\rightarrow$ keine Sicherheit in diesem Fall.

II.)
a)
$\phi(pq) = (p-1)(q-1)$
$\phi(47 \cdot 59) = (47-1)(59-1) = 46 \cdot 58 = 2668$

$2668 = 156 \cdot 17 + 16$
$17 = 1 \cdot 16 + 1$

Sie sind teilerfremd.

b)
Modulares Inverses von $e \mod \phi(pq) = 17 \mod 2668$
$d \cdot e \mod \phi(pq) = 1$
$d \cdot e + x \cdot \phi(pq) = 1$

$1 = 17 - 1 \cdot 16$
$1 = 17 - (2668 - 156 \cdot 17)$
$1 = 157 \cdot 17 + (-1) \cdot 2668$
$d = 157$

$$\begin{aligned} e\ d &\equiv 1 \mod \phi(pq) \\ 17 \cdot 157 &\equiv 1 \mod 2668 \\ 2669 &\equiv 1 \mod 2668 \end{aligned}$$

true

c)
$e : 17$
$n : 2773$
$m_1 : 8\ m_2 : 117\ m_3 : 1212$
$c \equiv m^e \mod n$

$$m_1 \to c_1 = 8^{17} \mod 2773 = 596$$
$$m_2 \to c_2 = 117^{17} \mod 2773 = 1769$$
$$m_3 \to c_3 = 1212^{17} \mod 2773 = 2345$$

d)
$d = 157$
$n = 2773$

$$c_1 \to m_1 = 596^{157} \mod 2773 = 8$$
$$c_2 \to m_2 = 1769^{157} \mod 2773 = 117$$
$$c_3 \to m_3 = 2345^{157} \mod 2773 = 1212$$

III.)
$n = 17'753$
$\phi(n) = 17280$

$\phi(n) = (p-1)(q-1)$
$n = p \cdot q \to q = \frac{n}{p}$

2 Unbekannte, 2 Gleichungen

$$\begin{aligned}
(p-1)(q-1) &= \phi(n) \\
(p-1)\left(\frac{n}{p} - 1\right) &= \phi(n) \\
n - p - \frac{n}{p} + 1 &= \phi(n) \\
n - p - \frac{n}{p} + 1 - \phi(n) &= 0 \\
-p^2 + np - n + p - \phi(n) \cdot p &= 0 \\
-p^2 + (n - \phi(n) + 1)p - n &= 0 \\
-p^2 + 474p - 17'753 &= 0
\end{aligned}$$

$p_1 = 41$
$p_2 = 433$

IV.)
Schlüssel: $(n, e) = (2537, 13)$
Geheimtext: $c = 2018$

n faktorisieren $\rightarrow n = 43 \cdot 59$
$\phi(n) = (43 - 1)(59 - 1) = 42 \cdot 58 = 2436$

Modular Inverse d von e mod $\phi(n)$
Mi erweitertertem euklidischem Algorithmus $\rightarrow d \cdot e + x \cdot \phi(n) = 1$

$1 = -5 \cdot 2436 + 937 \cdot 13$

Mit modulo rechnen und es folgt: $d \cdot e = 937 \cdot 13 \equiv 1 \mod 2436$
$d = 937$

Für Klartext berechnen, Formel: $M = C^d \mod n$ anwenden.
$M = C^d \mod n = 2081^{937} \mod 2537 = 1819$