Thursday 18th June, 2026

13:04

# An introduction to arithmetic-based cryptography: Cryptography Treasure Hunt BNTD 14

Bogdan Jones and Darius Jones

Abstract.

Contents



*Key words and phrases:* modular arithmetic, prime numbers

*2010 Mathematics Subject Classification:* 11G05, 11G20, 11N05 (Primary), 11N80 (Secondary)

A.C.C. was partially supported by a Collaboration Grant for Mathematicians from the Simons Foundation under Award No. 709008.

File started on July 3, 2024.

## 1. Caesar cipher

To encrypt an English letter message using the Caesar cipher,

- each letter in the English alphabet is **shifted to the left** as many spots as indicated by a given **shifting encryption key** $k \in \{0, 1, \ldots, 25\}$; the alphabet obtained by shifting the letters $k$ spots to the left is called **the Caesar alphabet with shifting encryption key** $k$
- using the above alphabet,

each plaintext letter in position $\ell$ is replaced with the ciphertext letter in position $\ell + k$.

To decrypt an English letter message encrypted using the Caesar cipher with shifting encryption key $k$,

- each ciphertext letter is **shifted to the right** as many spots as indicated by the shifting encryption key $k$, i.e.

each ciphertext letter in position $\mathcal{L}$ is replaced with the plaintext letter in position $\mathcal{L} - k$.

The integer $-k$ is called the **shifting decryption key of the Caesar cipher** with shifting encryption key $k$.

Below are some conversions of English plaintext into English ciphertext using the Caesar cipher with various encryption keys.

Encryption key $k = 0$

| plaintext | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ciphertext | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ |

Encryption key $k = 5$

| plaintext | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ciphertext | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | $A$ | $B$ | $C$ | $D$ | $E$ |

Encryption key $k = 15$

| plaintext | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ciphertext | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ | $O$ |

**Examples of encryption and decryption using the Caesar cipher**

• Encrypt the message

| $c$ | $a$ | $e$ | $s$ | $a$ | $r$ |
|---|---|---|---|---|---|

using the Caesar cipher with encryption key $k = 5$.

**Solution.**

| ↓ shift each plaintext letter 5 spots to the left | plaintext | $c$ | $a$ | $e$ | $s$ | $a$ | $r$ |
|---|---|---|---|---|---|---|---|
| | ciphertext | $H$ | $F$ | $J$ | $X$ | $F$ | $W$ |

• Decrypt the message

| $H$ | $N$ | $U$ | $M$ | $J$ | $W$ |
|---|---|---|---|---|---|

encrypted using the Caesar cipher with encryption key $k = 5$.

**Solution.**

Since the encryption key is $k = 5$, the decryption key is $-k = -5$.

| | plaintext | $c$ | $i$ | $p$ | $h$ | $e$ | $r$ |
|---|---|---|---|---|---|---|---|
| ↑ shift each ciphertext letter 5 spots to the right | ciphertext | $H$ | $N$ | $U$ | $M$ | $J$ | $W$ |

Indiciu 1 – Cifrul lui Caesar

LX NFWZLCPL DXLCLWOFWFT

**Solution.** $k =$

| English alphabet | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| English alphabet | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ |
| shifted English alphabet | | | | | | | | | | | | | | | | | | | | | | | | | | |

| plaintext | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ciphertext | $L$ | $X$ | | $N$ | $F$ | $W$ | $Z$ | $L$ | $C$ | $P$ | $L$ | | $D$ | $X$ | $L$ | $C$ | $L$ | $W$ | $O$ | $F$ | $W$ | $F$ | $T$ |

Indiciu 2 – Cifrul lui Caesar

JMTAFMD S AEHJMEMLSL FMSFLS EWS

**Solution.** $k =$

| English alphabet | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| English alphabet | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ |
| shifted English alphabet | | | | | | | | | | | | | | | | | | | | | | | | | | |

| plaintext | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ciphertext | $J$ | $M$ | $T$ | $A$ | $F$ | $M$ | $D$ | | $S$ | | $A$ | $E$ | $H$ | $J$ | $M$ | $E$ | $M$ | $L$ | $S$ | $L$ | | $F$ | $M$ | $S$ | $F$ | $L$ | $S$ | | $E$ | $W$ | $S$ |

## 2. Additive cipher

To encrypt an English letter message using the additive cipher,

- the letters in the English alphabet are replaced with the sequence of integers from 0 to 25, forming a **residue-letter alphabet**; the integers in the residue alphabet are called **residue-letters** and are written with a hat on top to indicate that they refer to residues modulo 26
- each residue-letter in the residue-letter alphabet is **shifted to the left** as many spots as indicated by a given **additive encryption key** $k_a \in \{0, 1, \ldots, 25\}$; the residue-letter alphabet obtained by shifting the residue-letters $k_a$ spots to the left is called **the additive residue-letter alphabet with additive encryption key** $k_a$
- using the above alphabet,

  each plaintext residue-letter $\widehat{\mathfrak{n}}$ is replaced with the ciphertext residue-letter $\widehat{\mathfrak{n} + k_a}$.

To decrypt an English letter message encrypted using the additive cipher with encryption key $k_a$,

- the residue class modulo 26 of the additive encryption key $k_a$ is subtracted from each ciphertext residue-letter, i.e.

  each ciphertext residue-letter $\widehat{\mathfrak{N}}$ is replaced with the plaintext residue-letter $\widehat{\mathfrak{N} - k_a}$

- the resulting plaintext residue-letters are converted into English letters.

The representative $-k_a \in \{0, -1, \ldots, -25\}$ is called the **additive decryption key of the additive cipher** with additive encryption key $k_a$.

Below is the English alphabet – residue-letter alphabet dictionary.

| English alphabet | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| residue-letter alphabet | $\widehat{0}$ | $\widehat{1}$ | $\widehat{2}$ | $\widehat{3}$ | $\widehat{4}$ | $\widehat{5}$ | $\widehat{6}$ | $\widehat{7}$ | $\widehat{8}$ | $\widehat{9}$ | $\widehat{10}$ | $\widehat{11}$ | $\widehat{12}$ | $\widehat{13}$ | $\widehat{14}$ | $\widehat{15}$ | $\widehat{16}$ | $\widehat{17}$ | $\widehat{18}$ | $\widehat{19}$ | $\widehat{20}$ | $\widehat{21}$ | $\widehat{22}$ | $\widehat{23}$ | $\widehat{24}$ | $\widehat{25}$ |

Below is a conversion of English plaintext into residue-letter ciphertext using the additive cipher with encryption key 5.

Encryption key $k_a = 5$

| plaintext | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ciphertext | $\widehat{5}$ | $\widehat{6}$ | $\widehat{7}$ | $\widehat{8}$ | $\widehat{9}$ | $\widehat{10}$ | $\widehat{11}$ | $\widehat{12}$ | $\widehat{13}$ | $\widehat{14}$ | $\widehat{15}$ | $\widehat{16}$ | $\widehat{17}$ | $\widehat{18}$ | $\widehat{19}$ | $\widehat{20}$ | $\widehat{21}$ | $\widehat{22}$ | $\widehat{23}$ | $\widehat{24}$ | $\widehat{25}$ | $\widehat{0}$ | $\widehat{1}$ | $\widehat{2}$ | $\widehat{3}$ | $\widehat{4}$ |

**Examples of encryption and decryption using the additive cipher**

• Encrypt the message

| $a$ | $d$ | $d$ | $i$ | $t$ | $i$ | $v$ | $e$ |
|---|---|---|---|---|---|---|---|

using the additive cipher with encryption key $k_a = 5$.

**Solution.**

| ↓ convert each letter into a residue-letter | plaintext | $a$ | $d$ | $d$ | $i$ | $t$ | $i$ | $v$ | $e$ |
|---|---|---|---|---|---|---|---|---|---|
| ↓ add $\widehat{5}$ to each residue-letter | plaintext in residue-letters | $\widehat{0}$ | $\widehat{3}$ | $\widehat{3}$ | $\widehat{8}$ | $\widehat{19}$ | $\widehat{8}$ | $\widehat{21}$ | $\widehat{4}$ |
| | ciphertext in residue-letters | $\widehat{5}$ | $\widehat{8}$ | $\widehat{8}$ | $\widehat{13}$ | $\widehat{24}$ | $\widehat{13}$ | $\widehat{0}$ | $\widehat{9}$ |

• Decrypt the message

| $\widehat{7}$ | $\widehat{13}$ | $\widehat{20}$ | $\widehat{12}$ | $\widehat{9}$ | $\widehat{22}$ |
|---|---|---|---|---|---|

encrypted using the additive cipher with encryption key $k_a = 5$.

**Solution.**

Since the encryption key is $k_a = 5$, the decryption key is $-k_a = -5$.

| | plaintext | $c$ | $i$ | $p$ | $h$ | $e$ | $r$ |
|---|---|---|---|---|---|---|---|
| ↑ convert each residue-letter into a letter | plaintext in residue-letters | $\widehat{2}$ | $\widehat{8}$ | $\widehat{15}$ | $\widehat{7}$ | $\widehat{4}$ | $\widehat{17}$ |
| ↑ subtract $\widehat{5}$ from each residue-letter | ciphertext in residue-letters | $\widehat{7}$ | $\widehat{13}$ | $\widehat{20}$ | $\widehat{12}$ | $\widehat{9}$ | $\widehat{22}$ |

Indiciu 3 – Cifrul Aditiv

21 20 25 14  01 10 09 10 06  06 08 10 06 24 25 06  25 10 19 25 06  14 19  24 06 11 14 23

**Solution.** $k_a =$

| English alphabet | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| residue-letter alphabet | $\widehat{0}$ | $\widehat{1}$ | $\widehat{2}$ | $\widehat{3}$ | $\widehat{4}$ | $\widehat{5}$ | $\widehat{6}$ | $\widehat{7}$ | $\widehat{8}$ | $\widehat{9}$ | $\widehat{10}$ | $\widehat{11}$ | $\widehat{12}$ | $\widehat{13}$ | $\widehat{14}$ | $\widehat{15}$ | $\widehat{16}$ | $\widehat{17}$ | $\widehat{18}$ | $\widehat{19}$ | $\widehat{20}$ | $\widehat{21}$ | $\widehat{22}$ | $\widehat{23}$ | $\widehat{24}$ | $\widehat{25}$ |
| additive residue-letter alphabet | | | | | | | | | | | | | | | | | | | | | | | | | | |

| plaintext | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| plaintext in residue-letters | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ciphertext in residue-letters | $\widehat{21}$ | $\widehat{20}$ | $\widehat{25}$ | $\widehat{14}$ | | $\widehat{1}$ | $\widehat{10}$ | $\widehat{9}$ | $\widehat{10}$ | $\widehat{6}$ | | $\widehat{6}$ | $\widehat{8}$ | $\widehat{10}$ | $\widehat{6}$ | $\widehat{24}$ | $\widehat{25}$ | $\widehat{6}$ | | $\widehat{14}$ | $\widehat{19}$ | | $\widehat{24}$ | $\widehat{6}$ | $\widehat{11}$ | $\widehat{14}$ | $\widehat{23}$ |

Indiciu 4 – Cifrul Aditiv

14 07 24 19 13 04 21 21  16 17  13 07 04  21 25 21  05 17 13 25 13 00 13

**Solution.** $k_a =$

| English alphabet | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| residue-letter alphabet | $\widehat{0}$ | $\widehat{1}$ | $\widehat{2}$ | $\widehat{3}$ | $\widehat{4}$ | $\widehat{5}$ | $\widehat{6}$ | $\widehat{7}$ | $\widehat{8}$ | $\widehat{9}$ | $\widehat{10}$ | $\widehat{11}$ | $\widehat{12}$ | $\widehat{13}$ | $\widehat{14}$ | $\widehat{15}$ | $\widehat{16}$ | $\widehat{17}$ | $\widehat{18}$ | $\widehat{19}$ | $\widehat{20}$ | $\widehat{21}$ | $\widehat{22}$ | $\widehat{23}$ | $\widehat{24}$ | $\widehat{25}$ |
| additive residue-letter alphabet | | | | | | | | | | | | | | | | | | | | | | | | | | |

| plaintext | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| plaintext in residue-letters | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ciphertext in residue-letters | $\widehat{14}$ | $\widehat{7}$ | $\widehat{24}$ | $\widehat{19}$ | $\widehat{13}$ | $\widehat{4}$ | $\widehat{21}$ | $\widehat{21}$ | | $\widehat{16}$ | $\widehat{17}$ | | $\widehat{13}$ | $\widehat{7}$ | $\widehat{4}$ | | $\widehat{21}$ | $\widehat{25}$ | $\widehat{21}$ | | $\widehat{5}$ | $\widehat{17}$ | $\widehat{13}$ | $\widehat{25}$ | $\widehat{13}$ | $\widehat{0}$ | $\widehat{13}$ |

## 3. Multiplicative cipher

To encrypt an English letter message using the multiplicative cipher,

- the letters in the English alphabet are replaced with the sequence of integers from 0 to 25, forming a **residue-letter alphabet**; the integers in the residue-letter alphabet are called **residue-letters** and are written with a hat on top to indicate that they refer to residues modulo 26
- each residue-letter in the residue-letter alphabet is replaced with the the residue modulo 26 of the product between the residue-letter and a given **multiplicative encryption key** $k_m \in \{0, 1, \ldots, 25\}$; the residue-letter alphabet obtained by multiplying the residue-letters by $k_m$ is called **the multiplicative residue-letter alphabet with multiplicative encryption key** $k_m$
- using the above alphabet,

  each plaintext residue-letter $\widehat{\mathfrak{n}}$ is replaced with the ciphertext residue-letter $\widehat{\mathfrak{n}k_m}$.

To decrypt an English letter message encrypted using the multiplicative cipher with encryption key $k_m$,

- each ciphertext residue-letter is multiplied by the multiplicative inverse modulo 26 of the multiplicative encryption key $k_m$, i.e.

  each ciphertext residue-letter $\widehat{\mathfrak{N}}$ is replaced with the plaintext residue-letter $\widehat{k_m^{-1}\mathfrak{N}}$

- the resulting plaintext residue-letters are converted into English letters.

The representative in $\{0, 1, \ldots, 25\}$ of $\widehat{k_m}^{-1}$ is called the **multiplicative decryption key of the multiplicative cipher** with multiplicative encryption key $k_m$.

**Warning:** the encryption multiplicative key $k_m$ must be chosen so that its multiplicative inverse modulo 26 exists.

Below is the English alphabet – residue-letter alphabet dictionary.

| English alphabet | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| residue-letter alphabet | $\widehat{0}$ | $\widehat{1}$ | $\widehat{2}$ | $\widehat{3}$ | $\widehat{4}$ | $\widehat{5}$ | $\widehat{6}$ | $\widehat{7}$ | $\widehat{8}$ | $\widehat{9}$ | $\widehat{10}$ | $\widehat{11}$ | $\widehat{12}$ | $\widehat{13}$ | $\widehat{14}$ | $\widehat{15}$ | $\widehat{16}$ | $\widehat{17}$ | $\widehat{18}$ | $\widehat{19}$ | $\widehat{20}$ | $\widehat{21}$ | $\widehat{22}$ | $\widehat{23}$ | $\widehat{24}$ | $\widehat{25}$ |

Below is a conversion of English plaintext into residue-letter ciphertext using the multiplicative cipher with encryption key 5.

Encryption key $k_m = 5$

| plaintext | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ciphertext | $\widehat{0}$ | $\widehat{5}$ | $\widehat{10}$ | $\widehat{15}$ | $\widehat{20}$ | $\widehat{25}$ | $\widehat{4}$ | $\widehat{9}$ | $\widehat{14}$ | $\widehat{19}$ | $\widehat{24}$ | $\widehat{3}$ | $\widehat{8}$ | $\widehat{13}$ | $\widehat{18}$ | $\widehat{23}$ | $\widehat{2}$ | $\widehat{7}$ | $\widehat{12}$ | $\widehat{17}$ | $\widehat{22}$ | $\widehat{1}$ | $\widehat{6}$ | $\widehat{11}$ | $\widehat{16}$ | $\widehat{21}$ |

**Examples of encryption and decryption using the multiplicative cipher**

• Encrypt the message

| $m$ | $u$ | $l$ | $t$ | $i$ | $p$ | $l$ | $i$ | $c$ | $a$ | $t$ | $i$ | $v$ | $e$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

using the multiplicative cipher with encryption key $k_m = 5$.

**Solution.**

| ↓ convert each letter into a residue-letter | plaintext | $m$ | $u$ | $l$ | $t$ | $i$ | $p$ | $l$ | $i$ | $c$ | $a$ | $t$ | $i$ | $v$ | $e$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↓ multiply each plaintext residue-letter by $\widehat{5}$ | plaintext in residue-letters | $\widehat{12}$ | $\widehat{20}$ | $\widehat{11}$ | $\widehat{19}$ | $\widehat{8}$ | $\widehat{15}$ | $\widehat{11}$ | $\widehat{8}$ | $\widehat{2}$ | $\widehat{0}$ | $\widehat{19}$ | $\widehat{8}$ | $\widehat{21}$ | $\widehat{4}$ |
| | ciphertext in residue-letters | $\widehat{8}$ | $\widehat{22}$ | $\widehat{3}$ | $\widehat{17}$ | $\widehat{14}$ | $\widehat{23}$ | $\widehat{3}$ | $\widehat{14}$ | $\widehat{10}$ | $\widehat{0}$ | $\widehat{17}$ | $\widehat{14}$ | $\widehat{1}$ | $\widehat{20}$ |

• Decrypt the message

| $\widehat{10}$ | $\widehat{14}$ | $\widehat{23}$ | $\widehat{9}$ | $\widehat{20}$ | $\widehat{7}$ |
|---|---|---|---|---|---|

encrypted using the multiplicative cipher with encryption key $k_m = 5$.

**Solution.**

Since the encryption key is $k_m = 5$ and $\gcd(26, k_m) = \gcd(26, 5) = 1$, the decryption key exists and is the representative in $\{0, 1, \ldots, 25\}$ of $\widehat{k_m}^{-1}$. We will show after this example that $\widehat{5}^{-1} = \widehat{21}$. Thus the decryption key is 21.

| | plaintext | $c$ | $i$ | $p$ | $h$ | $e$ | $r$ |
|---|---|---|---|---|---|---|---|
| ↑ convert each residue-letter into a letter | plaintext in residue-letters | $\widehat{2}$ | $\widehat{8}$ | $\widehat{15}$ | $\widehat{7}$ | $\widehat{4}$ | $\widehat{17}$ |
| ↑ multiply each ciphertext residue-letter by $\widehat{5}^{-1} = \widehat{21}$ | ciphertext in residue-letters | $\widehat{10}$ | $\widehat{14}$ | $\widehat{23}$ | $\widehat{9}$ | $\widehat{20}$ | $\widehat{7}$ |

• Use the euclidean algorithm to find $\widehat{5}^{-1}$.

**Solution.**

We use the notation $k_m = 5$.

**Step 1:** Use the euclidean algorithm to show that $\gcd(26, k_m) = 1$.

$$26 = 5 \cdot 5 + 1,$$

$$5 = 1 \cdot 5 + 0 \quad \text{STOP.}$$

**Step 2:** Rewrite all, but the last, equations of Step 1 as linear representations of the corresponding non-zero remainders.

$$1 = 26 + 5 \cdot (-5).$$

**Step 3:** Using the equations of Step 2 in reversed order, write $1 = 26 \cdot$ **integer** $+ k_m \cdot$ **integer**.

For $k_m = 5$, this was already achieved in Step 2:

$$1 = 26 \cdot 1 + 5 \cdot (-5).$$

**Step 4:** Reduce modulo 26 the equation $1 = 26 \cdot$ **integer** $+ k_m \cdot$ **integer** obtained in Step 3.

$$1 \equiv 5 \cdot (-5) (\mathrm{mod}\, 26).$$

**Step 5:** Use Step 4 to derive the inverse of $k_m$ modulo 26.

$$\widehat{5}^{-1} = \widehat{-5} = \widehat{26 - 5} = \widehat{21}.$$

Indicui 5 – Cifrul Multiplicativ

00 10 12 05 24 02 05 08 07  25 00 09 24 00 23 00  00 06 12 00 02 05 00  13 08 00 13 05 00

**Solution.** $k_m =$

| English alphabet | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| residue-letter alphabet | $\widehat{0}$ | $\widehat{1}$ | $\widehat{2}$ | $\widehat{3}$ | $\widehat{4}$ | $\widehat{5}$ | $\widehat{6}$ | $\widehat{7}$ | $\widehat{8}$ | $\widehat{9}$ | $\widehat{10}$ | $\widehat{11}$ | $\widehat{12}$ | $\widehat{13}$ | $\widehat{14}$ | $\widehat{15}$ | $\widehat{16}$ | $\widehat{17}$ | $\widehat{18}$ | $\widehat{19}$ | $\widehat{20}$ | $\widehat{21}$ | $\widehat{22}$ | $\widehat{23}$ | $\widehat{24}$ | $\widehat{25}$ |
| multiplicative residue-letter alphabet | | | | | | | | | | | | | | | | | | | | | | | | | | |

| plaintext | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| plaintext in residue-letters | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ciphertext in residue-letters | $\widehat{0}$ | $\widehat{10}$ | $\widehat{12}$ | $\widehat{5}$ | $\widehat{24}$ | $\widehat{2}$ | $\widehat{5}$ | $\widehat{8}$ | $\widehat{7}$ | | $\widehat{25}$ | $\widehat{0}$ | $\widehat{9}$ | $\widehat{24}$ | $\widehat{0}$ | $\widehat{23}$ | $\widehat{0}$ | | $\widehat{0}$ | $\widehat{6}$ | $\widehat{12}$ | $\widehat{0}$ | $\widehat{2}$ | $\widehat{5}$ | $\widehat{0}$ | | $\widehat{13}$ | $\widehat{8}$ | $\widehat{0}$ | $\widehat{13}$ | $\widehat{5}$ | $\widehat{0}$ |

## 4. RSA cipher

To encrypt an English letter message using the RSA cipher[1],

- the letters in the English alphabet are replaced with the sequence of two-digit numbers $\{00, 01, \ldots, 25\}$, forming a **two-digit letter alphabet** (note that this conversion is a variation of the one used in the Caesar, additive, multiplicative, and affine ciphers)
- the plaintext is converted into one single base ten number $\mathfrak{n}$, called **plaintext number**, by replacing each English letter in the plaintext with its corresponding double-digit number
- two distinct prime numbers $p_1$ and $p_2$ which do not divide $\mathfrak{n}$ are chosen and multiplied together to produce a composite integer $\mathfrak{m} := p_1 p_2$; the primes $p_1$, $p_2$ and the integer $\phi(\mathfrak{m}) := (p_1 - 1)(p_2 - 1)$ are kept secret
- a positive integer $\mathfrak{e}$ is chosen such that $\gcd(\mathfrak{e}, (p_1 - 1)(p_2 - 1)) = 1$
- the pair of integers $(\mathfrak{e}, \mathfrak{m})$ is made public and is called the **public encryption key**;
- the plaintext number $\mathfrak{n}$ is replaced with the representative between 0 and $\mathfrak{m} - 1$ of the residue class of $\mathfrak{n}^{\mathfrak{e}}$ modulo $\mathfrak{m}$, called the **ciphertext number**, i.e.

the plaintext number $\mathfrak{n}$ is replaced with the ciphertext number $\mathfrak{N} \in \{0, 1, \ldots, \mathfrak{m} - 1\}$, where $\mathfrak{N} \equiv \mathfrak{n}^{\mathfrak{e}} (\mathrm{mod}\, \mathfrak{m})$.

The ciphertext obtained this way is said to have been encrypted using

**the RSA cipher with public encryption key $(\mathfrak{e}, \mathfrak{m})$.**

To decrypt an English letter message encrypted as the ciphertext number $\mathfrak{N}$ using the RSA cipher with public encryption key $(\mathfrak{e}, \mathfrak{m})$,

- a positive integer $\mathfrak{d}$ such that $\mathfrak{d}\mathfrak{e} \equiv 1 (\mathrm{mod}\, \phi(\mathfrak{m}))$ must be found; the integer $\mathfrak{d}$ is called the **private decryption key of the RSA cipher** with public encryption key $(\mathfrak{e}, \mathfrak{m})$
- the plaintext number $\mathfrak{n}$ is obtained by raising the ciphertext number $\mathfrak{N}$ to $\mathfrak{d}$ and reducing the result modulo $\mathfrak{m}$, i.e.

the ciphertext number $\mathfrak{N}$ is replaced with the representative $\mathfrak{n}$ in $\{0, 1, \ldots, \mathfrak{m} - 1\}$ of $\mathfrak{N}^{\mathfrak{d}} (\mathrm{mod}\, \mathfrak{m})$

- the plaintext number $\mathfrak{n}$ is separated into two-digit letters, starting from the end and adding digit 0 at the beginning, if necessary
- the resulting two-digit letters are converted into English letters.

Below is the English alphabet – two-digit letter alphabet dictionary.

| English alphabet | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ | $s$ | $t$ | $u$ | $v$ | $w$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| two-digit alphabet | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

[1]The RSA cipher was invented by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977 and bears the initials of their last names. It was the first example of a feasible public key cryptosystem – an encryption system for which, in practice, it is difficult to derive the decryption key from the encryption key.

**Examples of encryption and decryption using the RSA cipher**

- Encrypt the message

| $r$ | $s$ | $a$ |
|---|---|---|

using the RSA cipher with public encryption key $(\mathfrak{e} = 7, \mathfrak{m} = 27452160653)$.

**Solution.**

| ↓ convert each letter into a double-digit letter | plaintext | $r\|s\|a$ |
|---|---|---|
| ↓ concatenate the double-digit letters into one number | plaintext in two-digit alphabet | 17\|18\|00 |
| ↓ raise the plaintext number to exponent $\mathfrak{e} = 7$ and reduce the result modulo $\mathfrak{m} = 27451829280$ | plaintext number | 171800 |
| | ciphertext number | 22462001934 |

- Decrypt the message

| 3795306647 |
|---|

encrypted using the RSA cipher with public encryption key $(\mathfrak{e} = 7, \mathfrak{m} = 27452160653)$ and private decryption key $\mathfrak{d} = 23530139383$. Since $\mathfrak{d}$ is large, it is not computationally feasible to actually compute $3795306647^{\mathfrak{d}}$ and then reduce modulo $\mathfrak{m}$; instead, start with the binary representation of $\mathfrak{d}$ as

$$\mathfrak{d} = 2^{34} + 2^{32} + 2^{30} + 2^{29} + 2^{28} + 2^{27} + 2^{25} + 2^{23} + 2^{16} + 2^{14} + 2^{13} + 2^{11} + 2^{10} + 2^9 + 2^7 + 2^6 + 2^5 + 2^4 + 2^2 + 2 + 1,$$

compute the powers

$$3795306647^{2^{34}} \pmod{\mathfrak{m}}, 3795306647^{2^{32}} \pmod{\mathfrak{m}}, 3795306647^{2^{30}} \pmod{\mathfrak{m}}, \ldots$$

by successive squaring modulo $\mathfrak{m}$ and then multiply them together modulo $\mathfrak{m}$, reducing modulo $\mathfrak{m}$ after every multiplication.

**Solution.**

| | plaintext | $c\|i\|p\|h\|e\|r$ |
|---|---|---|
| ↑ convert each double-digit letter into an English letter | plaintext in two-digit alphabet | 02\|08\|15\|07\|04\|17 |
| ↑ separate the plaintext number into two-digit letters, starting from the end, and add digit 0 at the beginning, if necessary | plaintext number | 20815070417 |
| ↑ raise the ciphertext number to exponent $\mathfrak{d} = 23530139383$ and reduce the result modulo $\mathfrak{m} = 27452160653$ | ciphertext number | 3795306647 |

This clue is for you to decrypt later.

To decrypt it, you will need the aid of a computer.

Do NOT decrypt it at this time.

Instead, go to claim your prize!

Team 1 – RSA cipher

RSA with public key of $(\mathfrak{e}, \mathfrak{m})$, where

$$\mathfrak{e} := 3,$$

$\mathfrak{m} :=$ 871114391061223731352046815685701248390420738846949050308412037930835626672216367012720736097069 3.

The ciphertext is:

25197523411805417542708674354221176126487591299380436718439669157471641961550904157907650788227 88

To decrypt it, the following number is useful:

Hint = 57044457419924486089773623655366214110581901024531817078210688294852529133303658996862464890324 65.

You may want to compute $\text{Hint}^2 (\text{mod}\, \mathfrak{m})$.

Some useful online resources:

To check the primality of a number (even a pretty large one): https://www.numberempire.com/primenumbers.php

For computing sums or products of large numbers to large moduli: https://sagecell.sagemath.org/

In order to decrypt the above ciphertext, you may need to do some computer programming...

**Send the solution to bogdan.felix.jones@gmail.com**

(Bogdan Jones)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA
- Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania

*Email address*, Bogdan Jones: bogdan.felix.jones@gmail.com

(Darius Jones)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 1313 SEO, Chicago, 60607, IL, USA

*Email address*, Darius Jones: darius.aidan.jones@gmail.com