9. Cryptography

Coding Technology
Objective: secure communication over a public channel.

Construct cryptography algorithms which present high complexity for the attacker, but which can easily be deciphered using the key.
Simple cyphers I

**Additive cypher.** If the size of the alphabet is $n$ (e.g. $n = 26$ for English texts),

$$E_k(x) = y = x + k \mod n,$$

where $k$ is the value of the key.

If $k$ is unknown, $k$ can be either guessed by trying (26 possibilities for the English alphabet).
Additive cypher. If the size of the alphabet is \( n \) (e.g. \( n = 26 \) for English texts),
\[
E_k(x) = y = x + k \mod n,
\]
where \( k \) is the value of the key.
If \( k \) is unknown, \( k \) can be either guessed by trying (26 possibilities for the English alphabet).

Linear cypher:
\[
E_k(x) = y = ax + b \mod n,
\]
where \( k = (a, b) \) is the value of the key. \( \gcd(a, n) = 1 \) must hold!
Simple cyphers I

**Additive cypher.** If the size of the alphabet is $n$ (e.g. $n = 26$ for English texts),

$$E_k(x) = y = x + k \mod n,$$

where $k$ is the value of the key.

If $k$ is unknown, $k$ can be either guessed by trying (26 possibilities for the English alphabet).

**Linear cypher:**

$$E_k(x) = y = ax + b \mod n,$$

where $k = (a, b)$ is the value of the key. $\gcd(a, n) = 1$ must hold!

Decryption is also linear:

$$D_k(y) = a^{-1}y - a^{-1}b \mod n.$$

If the key is unknown, statistical analysis can help in guessing.
Problem 1

Decipher the cyphertext HYHUBERGB, encrypted by an additive cypher $y = x + k \mod 26$. 
Problem 1

Decipher the cyphertext HYHUBERGB, encrypted by an additive cypher $y = x + k \mod 26$.

Solution. Guess $k$ by trying:

- $k = 1$: HYHUBERGB $\rightarrow$ GXGTAADQFA;
Problem 1

Decipher the cyphertext HYHUBERGB, encrypted by an additive cypher $y = x + k \mod 26$.

Solution. Guess $k$ by trying:

- $k = 1$: HYHUBERGB $\rightarrow$ GXGTAQQFA;
- $k = 2$: HYHUBERGB $\rightarrow$ FWFSZCPEZ;
Problem 1

Decipher the cyphertext HYHUBERGB, encrypted by an additive cypher $y = x + k \mod 26$.

Solution. Guess $k$ by trying:

- $k = 1$: HYHUBERGB $\rightarrow$ GXGTADQFA;
- $k = 2$: HYHUBERGB $\rightarrow$ FWFSZCPEZ;
- $k = 3$: HYHUBERGB $\rightarrow$ EVERYBODY. ✓
Problem 2

Decypher the following cyphertext if we know that linear encryption is used.

FMXVEDKAPHERBNDKRXRSREFMORU
DSDKDVSHVUFEDKAPRKDLYEVLHRHHRH
Problem 2

Decypher the following cyphertext if we know that linear encryption is used.

FMXVEDKAPHFERBNDKRXRSREFMORU
DSDKDVSHVUFEDKAPRKDLYEVRHLHRH

Solution. We use statistical analysis.

<table>
<thead>
<tr>
<th>letter</th>
<th>prob.</th>
<th>letter</th>
<th>prob.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>.082</td>
<td>N</td>
<td>.067</td>
</tr>
<tr>
<td>B</td>
<td>.015</td>
<td>O</td>
<td>.075</td>
</tr>
<tr>
<td>C</td>
<td>.028</td>
<td>P</td>
<td>.019</td>
</tr>
<tr>
<td>D</td>
<td>.043</td>
<td>Q</td>
<td>.001</td>
</tr>
<tr>
<td>E</td>
<td>.127</td>
<td>R</td>
<td>.060</td>
</tr>
<tr>
<td>F</td>
<td>.022</td>
<td>S</td>
<td>.063</td>
</tr>
<tr>
<td>G</td>
<td>.020</td>
<td>T</td>
<td>.091</td>
</tr>
<tr>
<td>H</td>
<td>.061</td>
<td>U</td>
<td>.028</td>
</tr>
<tr>
<td>I</td>
<td>.070</td>
<td>V</td>
<td>.010</td>
</tr>
<tr>
<td>J</td>
<td>.002</td>
<td>W</td>
<td>.023</td>
</tr>
<tr>
<td>K</td>
<td>.008</td>
<td>X</td>
<td>.001</td>
</tr>
<tr>
<td>L</td>
<td>.040</td>
<td>Y</td>
<td>.020</td>
</tr>
<tr>
<td>M</td>
<td>.024</td>
<td>Z</td>
<td>.001</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>letter</th>
<th>freq.</th>
<th>letter</th>
<th>freq.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2</td>
<td>N</td>
<td>1</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>O</td>
<td>1</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>P</td>
<td>2</td>
</tr>
<tr>
<td>D</td>
<td>7</td>
<td>Q</td>
<td>0</td>
</tr>
<tr>
<td>E</td>
<td>5</td>
<td>R</td>
<td>8</td>
</tr>
<tr>
<td>F</td>
<td>4</td>
<td>S</td>
<td>3</td>
</tr>
<tr>
<td>G</td>
<td>0</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>H</td>
<td>5</td>
<td>U</td>
<td>2</td>
</tr>
<tr>
<td>I</td>
<td>0</td>
<td>V</td>
<td>4</td>
</tr>
<tr>
<td>J</td>
<td>0</td>
<td>W</td>
<td>0</td>
</tr>
<tr>
<td>K</td>
<td>5</td>
<td>X</td>
<td>2</td>
</tr>
<tr>
<td>L</td>
<td>2</td>
<td>Y</td>
<td>1</td>
</tr>
<tr>
<td>M</td>
<td>2</td>
<td>Z</td>
<td>0</td>
</tr>
</tbody>
</table>
Problem 2

In the cyphertext, the most frequent letters are: R(8), D(7), E(5), H(5), K(5).

These are good candidates for E and T (the two most frequent letters in English texts).
Problem 2

In the cyphertext, the most frequent letters are: R(8), D(7), E(5), H(5), K(5).

These are good candidates for E and T (the two most frequent letters in English texts).

Guess 1: R → E, D → T. Then $E_k(4) = 17$, and $E_k(19) = 3$, that is,

\begin{align*}
4a + b &= 17 \mod 26, \\
19a + b &= 3 \mod 26.
\end{align*}
Problem 2

In the cyphertext, the most frequent letters are: R(8), D(7), E(5), H(5), K(5).

These are good candidates for E and T (the two most frequent letters in English texts).

Guess 1: R → E, D → T. Then $E_k(4) = 17$, and $E_k(19) = 3$, that is,

$$4a + b = 17 \quad \text{mod } 26,$$
$$19a + b = 3 \quad \text{mod } 26.$$

Subtraction gives

$$15a = 12 \quad \text{mod } 26,$$

but then $a$ must be even, so $\gcd(a, 26) > 1 \rightarrow$ incorrect guess.
Guess 2: $R \rightarrow E, E \rightarrow T$. Then

\[ 4a + b = 17 \pmod{26}, \]
\[ 19a + b = 4 \pmod{26}. \]

Then

\[ 15a = 13 \pmod{26}, \]
\[ a = 13 \pmod{26}, \]

so $\gcd(a, 26) > 1$ again $\rightarrow$ incorrect guess.
Problem 2

Guess 3: R → E, K → T. Then

\[4a + b = 17 \mod 26,\]
\[19a + b = 10 \mod 26.\]

Then

\[15a = 19 \mod 26,\]
\[a = 3 \mod 26,\]
\[b = 5 \mod 26.\]

\(k = (3, 5)\) is a valid key.
Problem 2

Guess 3: R → E, K → T. Then

\[ 4a + b = 17 \mod 26, \]
\[ 19a + b = 10 \mod 26. \]

Then

\[ 15a = 19 \mod 26, \]
\[ a = 3 \mod 26, \]
\[ b = 5 \mod 26. \]

\( k = (3, 5) \) is a valid key. We still need to check if we get meaningful decrypted text.

\[ D_k(y) = 3^{-1}y - 3^{-1} \cdot 5 = 9y - 19 \mod 26. \]

ALGORITHMS ARE QUITE GENERAL DEFINITIONS OF ARITHMETIC PROCESSES
Simple cyphers II

**Permutation cypher**: the message is cut into blocks of equal length, and the letters within each block are reordered according to the key permutation.

Example.

\[
\begin{array}{c}
1234567 \\
2147356
\end{array}
\iff
(12)(34765)
\]

Cypher: MORNING $\rightarrow$ OMIRNGN
Simple cyphers II

**Permutation cypher:** the message is cut into blocks of equal length, and the letters within each block are reordered according to the key permutation.

Example.

```
1234567  \leftrightarrow  (12)(34765)
2147356
```

Cypher: MORNING → OMIRNGN

**One time pad (OTP):** both the sender and the receiver have the same random bit sequence $k$; the encryption is bitwise addition of the message and the key. Example:

\[
\begin{align*}
x & = 01001101 01011101 \ldots \\
+k & = 11010000 11101011 \ldots \\
y & = 10011101 10110110 \ldots
\end{align*}
\]

As long as the key is used only once, OTP offers perfect secrecy. (Also, it is essentially the only such method.)
Problem 3

Using OTP encryption with key $k = (110011000001111)$, we receive the cyphertext $y = (011100010100011)$. Compute the plaintext $c$. 

Solution.

$$x = y + k \mod 2,$$

so 

$$y = 011100010100011 + k = 110011000001111$$

$$x = 101111010101100$$
Problem 3

Using OTP encryption with key \( k = (110011000001111) \), we receive the cyphertext \( y = (011100010100011) \). Compute the plaintext \( c \).

Solution. \( x = y + k \mod 2 \), so

\[
\begin{align*}
y & = 011100010100011 \\
+k & = 110011000001111 \\
\hline
x & = 101111010101100
\end{align*}
\]
Problem 4 – OTP without key exchange

A and B want to communicate using OTP without a common secret key. Assume A has key $k_A$ and B has key $k_B$. A has a message $x$ to send; he sends the message $y_1 = x + k_A$ to B, then B returns $y_2 = y_1 + k_B$, finally, A returns $y_3 = y_2 + k_A$. From the information

$$y_1 = (0111000100), \quad y_2 = (1000100100), \quad y_3 = (1000111011),$$

derive the plain text $x$ and keys $k_A$ and $k_B$. 

Problem 4 – OTP without key exchange

A and B want to communicate using OTP without a common secret key. Assume A has key $k_A$ and B has key $k_B$. A has a message $x$ to send; he sends the message $y_1 = x + k_A$ to B, then B returns $y_2 = y_1 + k_B$, finally, A returns $y_3 = y_2 + k_A$. From the information

\[ y_1 = (0111000100), \quad y_2 = (1000100100), \quad y_3 = (1000111011), \]

derive the plain text $x$ and keys $k_A$ and $k_B$.

Solution.

\[ y_1 = x + k_A, \quad y_2 = x + k_A + k_B, \quad y_3 = x + k_B \]

\[ y_1 + y_2 + y_3 = x + k_A + x + k_A + k_B + x + k_B = x. \]

From this,

\[ x = y_1 + y_2 + y_3 = (0111011011), \]

\[ k_A = x + y_1 = (0000011111), \]

\[ k_B = x + y_3 = (1111100000). \]
Problem 4 – OTP without key exchange

A and B want to communicate using OTP without a common secret key. Assume A has key $k_A$ and B has key $k_B$. A has a message $x$ to send; he sends the message $y_1 = x + k_A$ to B, then B returns $y_2 = y_1 + k_B$, finally, A returns $y_3 = y_2 + k_A$. From the information

\[ y_1 = (0111000100), \quad y_2 = (1000100100), \quad y_3 = (1000111011), \]

derive the plain text $x$ and keys $k_A$ and $k_B$.

Solution.

\[ y_1 = x + k_A, \quad y_2 = x + k_A + k_B, \quad y_3 = x + k_B \]

From this,

\[ x = y_1 + y_2 + y_3 = (0111011011), \]
\[ k_A = x + y_1 = (0000011111), \]
\[ k_B = x + y_3 = (1111100000). \]
Problem 4 – OTP without key exchange

A and B want to communicate using OTP without a common secret key. Assume A has key $k_A$ and B has key $k_B$. A has a message $x$ to send; he sends the message $y_1 = x + k_A$ to B, then B returns $y_2 = y_1 + k_B$, finally, A returns $y_3 = y_2 + k_A$. From the information

$$y_1 = (0111000100), \quad y_2 = (1000100100), \quad y_3 = (1000111011),$$

derive the plain text $x$ and keys $k_A$ and $k_B$.

Solution.

$$y_1 = x + k_A, \quad y_2 = x + k_A + k_B, \quad y_3 = x + k_B$$

$$y_1 + y_2 + y_3 = x + k_A + x + k_A + k_B + x + k_B = x.$$
Problem 4 – OTP without key exchange

A and B want to communicate using OTP without a common secret key. Assume A has key $k_A$ and B has key $k_B$. A has a message $x$ to send; he sends the message $y_1 = x + k_A$ to B, then B returns $y_2 = y_1 + k_B$, finally, A returns $y_3 = y_2 + k_A$. From the information

\[ y_1 = (0111000100), \quad y_2 = (1000100100), \quad y_3 = (1000111011), \]

derive the plain text $x$ and keys $k_A$ and $k_B$.

Solution.

\[ y_1 = x + k_A, \quad y_2 = x + k_A + k_B, \quad y_3 = x + k_B \]
\[ y_1 + y_2 + y_3 = x + k_A + x + k_A + k_B + x + k_B = x. \]

From this,

\[ x = y_1 + y_2 + y_3 = (0111011011), \]
\[ k_A = x + y_1 = (0000011111), \]
\[ k_B = x + y_3 = (1111100000). \]
Problem 5 – stochastic encryption

For stochastic encryption, the key \( k \) is chosen randomly. The plaintext \( \rightarrow \) cyphertext assignment depends on the key.

Consider the following setup:

▶ the space of the plaintext is \{a,b\} with probabilities \( P(a) = \frac{1}{3}, P(b) = \frac{2}{3} \).
▶ the space of the cyphertext is \{1,2,3,4,5\}.
▶ the keys are \{1,2,3,4,5\}, chosen with probabilities \{\frac{2}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}\} respectively.

The plaintext \( \rightarrow \) cyphertext assignment is the following:

\( k = 1 \):
\( a \rightarrow 1 \), \( b \rightarrow 2 \)

\( k = 2 \):
\( a \rightarrow 2 \), \( b \rightarrow 4 \)

\( k = 3 \):
\( a \rightarrow 3 \), \( b \rightarrow 1 \)

\( k = 4 \):
\( a \rightarrow 5 \), \( b \rightarrow 3 \)

\( k = 5 \):
\( a \rightarrow 4 \), \( b \rightarrow 5 \)

(a) Compute the cyphertext distribution.
(b) Are the plaintext and cyphertext independent (is this a perfect encryption)?
Problem 5 – stochastic encryption

For stochastic encryption, the key $k$ is chosen randomly. The plaintext → cyphertext assignment depends on the key. Consider the following setup:

- the space of the plaintext is $\{a, b\}$ with probabilities $\Pr(a) = 1/3, \Pr(b) = 2/3$.
- the space of the cyphertext is $\{1, 2, 3, 4, 5\}$.
- the keys are $\{1, 2, 3, 4, 5\}$, chosen with probability $\{2/5, 1/5, 1/5, 1/10, 1/10\}$ respectively.

(a) Compute the cyphertext distribution.
(b) Are the plaintext and cyphertext independent (is this a perfect encryption)?
Problem 5 – stochastic encryption

For stochastic encryption, the key $k$ is chosen randomly. The plaintext $\rightarrow$ cyphertext assignment depends on the key. Consider the following setup:

- the space of the plaintext is $\{a, b\}$ with probabilities $\Pr(a) = 1/3$, $\Pr(b) = 2/3$.
- the space of the cyphertext is $\{1, 2, 3, 4, 5\}$.
- the keys are $\{1, 2, 3, 4, 5\}$, chosen with probability $\{2/5, 1/5, 1/5, 1/10, 1/10\}$ respectively.

The plaintext $\rightarrow$ cyphertext assignment is the following:

\[
\begin{align*}
  k = 1 : & \quad a \rightarrow 1 \quad b \rightarrow 2 \\
  k = 2 : & \quad a \rightarrow 2 \quad b \rightarrow 4 \\
  k = 3 : & \quad a \rightarrow 3 \quad b \rightarrow 1 \\
  k = 4 : & \quad a \rightarrow 5 \quad b \rightarrow 3 \\
  k = 5 : & \quad a \rightarrow 4 \quad b \rightarrow 5
\end{align*}
\]
Problem 5 – stochastic encryption

For stochastic encryption, the key $k$ is chosen randomly. The plaintext $\rightarrow$ cyphertext assignment depends on the key. Consider the following setup:

- the space of the plaintext is $\{a,b\}$ with probabilities $\Pr(a) = 1/3, \Pr(b) = 2/3$.
- the space of the cyphertext is $\{1,2,3,4,5\}$.
- the keys are $\{1,2,3,4,5\}$, chosen with probability $\{2/5, 1/5, 1/5, 1/10, 1/10\}$ respectively.

The plaintext $\rightarrow$ cyphertext assignment is the following:

- $k = 1$: $a \rightarrow 1 \quad b \rightarrow 2$
- $k = 2$: $a \rightarrow 2 \quad b \rightarrow 4$
- $k = 3$: $a \rightarrow 3 \quad b \rightarrow 1$
- $k = 4$: $a \rightarrow 5 \quad b \rightarrow 3$
- $k = 5$: $a \rightarrow 4 \quad b \rightarrow 5$

(a) Compute the cyphertext distribution.
(b) Are the plaintext and cyphertext independent (is this a perfect encryption)?
Problem 5 – stochastic encryption

Solution.

(a) The cyphertext distribution can be computed using total probability:

\[ \Pr(Y = 1) = \Pr(Y = 1|X = a) \Pr(X = a) + \Pr(Y = 1|X = b) \Pr(X = b) = \]
\[ = \frac{2}{5} \cdot \frac{1}{3} + \frac{1}{5} \cdot \frac{2}{3} = \frac{4}{15} = 0.2667 \]
\[ \Pr(Y = 2) = \Pr(Y = 2|X = a) \Pr(X = a) + \Pr(Y = 2|X = b) \Pr(X = b) = \]
\[ = \frac{1}{5} \cdot \frac{1}{3} + \frac{2}{5} \cdot \frac{2}{3} = \frac{5}{15} = 0.3333 \]
\[ \Pr(Y = 3) = \Pr(Y = 3|X = a) \Pr(X = a) + \Pr(Y = 3|X = b) \Pr(X = b) = \]
\[ = \frac{1}{5} \cdot \frac{1}{3} + \frac{1}{10} \cdot \frac{2}{3} = \frac{4}{30} = 0.1333 \]
\[ \Pr(Y = 4) = \Pr(Y = 4|X = a) \Pr(X = a) + \Pr(Y = 4|X = b) \Pr(X = b) = \]
\[ = \frac{1}{10} \cdot \frac{1}{3} + \frac{1}{5} \cdot \frac{2}{3} = \frac{5}{30} = 0.1667 \]
\[ \Pr(Y = 5) = \Pr(Y = 5|X = a) \Pr(X = a) + \Pr(Y = 5|X = b) \Pr(X = b) = \]
\[ = \frac{1}{10} \cdot \frac{1}{3} + \frac{1}{10} \cdot \frac{2}{3} = \frac{1}{10} = 0.1 \]
Problem 5 – stochastic encryption

Solution.

(a) The cyphertext distribution can be computed using total probability:

\[
\begin{align*}
\Pr(Y = 1) &= \Pr(Y = 1|X = a) \Pr(X = a) + \Pr(Y = 1|X = b) \Pr(X = b) = \\
&= 2/5 \cdot 1/3 + 1/5 \cdot 2/3 = 4/15 = 0.2667 \\
\Pr(Y = 2) &= \Pr(Y = 2|X = a) \Pr(X = a) + \Pr(Y = 2|X = b) \Pr(X = b) = \\
&= 1/5 \cdot 1/3 + 2/5 \cdot 2/3 = 5/15 = 0.3333 \\
\Pr(Y = 3) &= \Pr(Y = 3|X = a) \Pr(X = a) + \Pr(Y = 3|X = b) \Pr(X = b) = \\
&= 1/5 \cdot 1/3 + 1/10 \cdot 2/3 = 4/30 = 0.1333 \\
\Pr(Y = 4) &= \Pr(Y = 4|X = a) \Pr(X = a) + \Pr(Y = 4|X = b) \Pr(X = b) = \\
&= 1/10 \cdot 1/3 + 1/5 \cdot 2/3 = 5/30 = 0.1667 \\
\Pr(Y = 5) &= \Pr(Y = 5|X = a) \Pr(X = a) + \Pr(Y = 5|X = b) \Pr(X = b) = \\
&= 1/10 \cdot 1/3 + 1/10 \cdot 2/3 = 1/10 = 0.1
\end{align*}
\]

(b) No, e.g.

\[
\Pr(Y = 1|X = a) = 2/5 \neq \Pr(Y = 1|X = b) = 1/5.
\]
Extended Euclidean Algorithm

The Extended Euclidean Algorithm can be used to find \( \gcd(a, b) \) and also to solve

\[
\gcd(a, b) = s \cdot a + t \cdot b.
\]
**Extended Euclidean Algorithm**

The Extended Euclidean Algorithm can be used to find \( \gcd(a, b) \) and also to solve

\[
\gcd(a, b) = s \cdot a + t \cdot b.
\]

Assume \( a > b \); initialize \( r_0 = a, r_1 = b \) and also \( s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1 \). In each step, we write

\[
r_{k-1} = r_k \cdot q_{k+1} + r_{k+1} \\
r_k = s_k \cdot a + t_k \cdot b,
\]

where \( 0 \leq r_{k+1} < r_k \), and \( s_{k+1} \) and \( t_{k+1} \) are computed from

\[
s_{k+1} = s_{k-1} - q_k s_k, \\
t_{k+1} = t_{k-1} - q_k t_k.
\]
The Extended Euclidean Algorithm can be used to find \( \gcd(a, b) \) and also to solve \( \gcd(a, b) = s \cdot a + t \cdot b \).

Assume \( a > b \); initialize \( r_0 = a, r_1 = b \) and also \( s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1 \). In each step, we write

\[
  r_{k-1} = r_k \cdot q_{k+1} + r_{k+1} \\
r_k = s_k \cdot a + t_k \cdot b,
\]

where \( 0 \leq r_{k+1} < r_k \), and \( s_{k+1} \) and \( t_{k+1} \) are computed from

\[
  s_{k+1} = s_{k-1} - q_k s_k, \\
t_{k+1} = t_{k-1} - q_k t_k.
\]

The algorithm stops when \( r_{k+1} = 0 \); then \( r_k = \gcd(a, b) \), and \( \gcd(a, b) = s_k \cdot a + t_k \cdot b \); at most \( \log_{1.62}(\min(a, b)) \) steps are needed.
Extended Euclidean Algorithm

The Extended Euclidean Algorithm can be used to find \( \gcd(a, b) \) and also to solve

\[
\gcd(a, b) = s \cdot a + t \cdot b.
\]

Assume \( a > b \); initialize \( r_0 = a, r_1 = b \) and also \( s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1 \). In each step, we write

\[
 r_{k-1} = r_k \cdot q_{k+1} + r_{k+1} \quad r_k = s_k \cdot a + t_k \cdot b,
\]

where \( 0 \leq r_{k+1} < r_k \), and \( s_{k+1} \) and \( t_{k+1} \) are computed from

\[
 s_{k+1} = s_{k-1} - q_k s_k, \quad t_{k+1} = t_{k-1} - q_k t_k.
\]

The algorithm stops when \( r_{k+1} = 0 \); then \( r_k = \gcd(a, b) \), and \( \gcd(a, b) = s_k \cdot a + t_k \cdot b \); at most \( \log_{1.62}(\min(a, b)) \) steps are needed.

For \( \gcd(n, e) = 1 \), the algorithm gives \( 1 = \gcd(n, e) = s \cdot n + t \cdot e \), so \( e^{-1} = t \mod n \).
Problem 5

Compute the greatest common divisor (gcd) of $b = 8387$ and $c = 1243$, and also compute $s$ and $t$ so that

$$\gcd(8387, 1243) = s \cdot 8387 + t \cdot 1243.$$
Problem 5

Compute the greatest common divisor \((\text{gcd})\) of \(b = 8387\) and \(c = 1243\), and also compute \(s\) and \(t\) so that

\[
\text{gcd}(8387, 1243) = s \cdot 8387 + t \cdot 1243.
\]

Solution.

\[
8387 = 1243 \cdot 6 + 929 \quad 929 = b - 6c
\]
Problem 5

Compute the greatest common divisor (gcd) of \( b = 8387 \) and \( c = 1243 \), and also compute \( s \) and \( t \) so that

\[
gcd(8387, 1243) = s \cdot 8387 + t \cdot 1243.
\]

Solution.

\[
\begin{align*}
8387 & = 1243 \cdot 6 + 929 \\
1243 & = 929 \cdot 1 + 314
\end{align*}
\]

\[
\begin{align*}
929 & = b - 6c \\
314 & = -b + 7c
\end{align*}
\]
Problem 5

Compute the greatest common divisor (gcd) of $b = 8387$ and $c = 1243$, and also compute $s$ and $t$ so that

$$\text{gcd}(8387, 1243) = s \cdot 8387 + t \cdot 1243.$$ 

Solution.

<table>
<thead>
<tr>
<th>$b$</th>
<th>$c$</th>
<th>$s$</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8387</td>
<td>1243</td>
<td>6</td>
<td>929</td>
</tr>
<tr>
<td>1243</td>
<td>929</td>
<td>1</td>
<td>314</td>
</tr>
<tr>
<td>929</td>
<td>314</td>
<td>2</td>
<td>301</td>
</tr>
<tr>
<td>301</td>
<td>13</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Finally, $\text{gcd}(8387, 1243) = -574 \cdot 8387 + 3873 \cdot 1243$. 
Problem 5

Compute the greatest common divisor (gcd) of $b = 8387$ and $c = 1243$, and also compute $s$ and $t$ so that

$$\text{gcd}(8387, 1243) = s \cdot 8387 + t \cdot 1243.$$ 

Solution.

\[
\begin{align*}
8387 &= 1243 \cdot 6 + 929 & 929 &= b - 6c \\
1243 &= 929 \cdot 1 + 314 & 314 &= -b + 7c \\
929 &= 314 \cdot 2 + 301 & 301 &= 3b - 20c \\
314 &= 301 \cdot 1 + 13 & 13 &= -4b + 27c
\end{align*}
\]
Problem 5

Compute the greatest common divisor (gcd) of $b = 8387$ and $c = 1243$, and also compute $s$ and $t$ so that

$$\gcd(8387, 1243) = s \cdot 8387 + t \cdot 1243.$$ 

Solution.

\[
\begin{align*}
8387 &= 1243 \cdot 6 + 929 & 929 &= b - 6c \\
1243 &= 929 \cdot 1 + 314 & 314 &= -b + 7c \\
929 &= 314 \cdot 2 + 301 & 301 &= 3b - 20c \\
314 &= 301 \cdot 1 + 13 & 13 &= -4b + 27c \\
301 &= 13 \cdot 23 + 2 & 2 &= 95b - 641c
\end{align*}
\]
Problem 5

Compute the greatest common divisor (gcd) of \( b = 8387 \) and \( c = 1243 \), and also compute \( s \) and \( t \) so that

\[
\gcd(8387, 1243) = s \cdot 8387 + t \cdot 1243.
\]

Solution.

\[
\begin{align*}
8387 & = 1243 \cdot 6 + 929 \\
1243 & = 929 \cdot 1 + 314 \\
929 & = 314 \cdot 2 + 301 \\
314 & = 301 \cdot 1 + 13 \\
301 & = 13 \cdot 23 + 2 \\
13 & = 2 \cdot 6 + 1
\end{align*}
\]

\[
\begin{align*}
929 & = b - 6c \\
314 & = -b + 7c \\
301 & = 3b - 20c \\
13 & = -4b + 27c \\
2 & = 95b - 641c \\
1 & = -574b + 3873c
\end{align*}
\]
Problem 5

Compute the greatest common divisor (gcd) of $b = 8387$ and $c = 1243$, and also compute $s$ and $t$ so that

$$\text{gcd}(8387, 1243) = s \cdot 8387 + t \cdot 1243.$$ 

Solution.

\[
\begin{align*}
8387 &= 1243 \cdot 6 + 929 \\
1243 &= 929 \cdot 1 + 314 \\
929 &= 314 \cdot 2 + 301 \\
314 &= 301 \cdot 1 + 13 \\
301 &= 13 \cdot 23 + 2 \\
13 &= 2 \cdot 6 + 1 \\
2 &= 1 \cdot 2 + 0.
\end{align*}
\]

Finally,

$$\text{gcd}(8387, 1243) = -574 \cdot 8387 + 3873 \cdot 1243.$$
Public key cryptography

Instead of a common key $k$ which is known by both the sender and the receiver, public key cryptography works the following way:

- the receiver has a $(d, e)$ pair of keys
- $d$ is a private key known only by the receiver
- $e$ is a public key known by everyone
RSA algorithm

The steps of the RSA algorithm are the following:

▶ Key generation:
  ▶ select 2 large primes $p$ and $q$; $n = pq$.
  ▶ $\phi(n) = (p - 1)(q - 1)$.
  ▶ Select a coding exponent $e$ so that $\gcd(e, \phi(n)) = 1$ and $1 < e < \phi(n)$.
  ▶ Solve $de = 1 \mod m$ to obtain the decoding key $d$.
  ▶ $(n, e)$ is the public key;
  ▶ $p, q, \phi(n)$ and $d$ are kept secret.

▶ Encryption (using the public key):
  ▶ the plaintext is cut into sections which can be turned into numbers $x$ such that $0 \leq x < n$.
  ▶ the cyphertext is $c = x^e \mod n$.

▶ Decryption:
  ▶ $x = c^d \mod n$. 
The steps of the RSA algorithm are the following:

- **Key generation:**
  - select 2 large primes $p$ and $q$; $n = pq$.
  - $\phi(n) = (p - 1)(q - 1)$.
  - Select a coding exponent $e$ so that $\gcd(e, \phi(n)) = 1$ and $1 < e < \phi(n)$.
  - Solve $de = 1 \mod m$ to obtain the decoding key $d$.
  - $(n, e)$ is the public key;
  - $p$, $q$, $\phi(n)$ and $d$ are kept secret.

- **Encryption (using the public key):**
  - the plaintext is cut into sections which can be turned into numbers $x$ such that $0 \leq x < n$.
  - the cyphertext is $c = x^e \mod n$. 
RSA algorithm

The steps of the RSA algorithm are the following:

▶ Key generation:
  ▶ select 2 large primes $p$ and $q$; $n = pq$.
  ▶ $\phi(n) = (p - 1)(q - 1)$.
  ▶ Select a coding exponent $e$ so that $\gcd(e, \phi(n)) = 1$ and $1 < e < \phi(n)$.
  ▶ Solve $de = 1 \mod m$ to obtain the decoding key $d$.
  ▶ $(n, e)$ is the public key;
  ▶ $p, q, \phi(n)$ and $d$ are kept secret.

▶ Encryption (using the public key):
  ▶ the plaintext is cut into sections which can be turned into numbers $x$ such that $0 \leq x < n$.
  ▶ the cyphertext is $c = x^e \mod n$.

▶ Decryption:
  ▶ $x = c^d \mod n$. 
Why does the RSA algorithm work?

Key generation is easy:

▶ Primality testing (checking whether a given number is a prime or not) is computationally fast.
▶ There are many primes even among large numbers: the Prime Number Theorem says that among numbers of order $N$, on average 1 out of $\log(N)$ numbers is a prime.
▶ So we can just start prime checking large numbers randomly, and we will eventually find two primes for $p$ and $q$.
▶ $\gcd$ and $\text{de} = 1 \mod \phi(n)$ can be solved fast using the Extended Euclidean Algorithm.
RSA algorithm

Why does the RSA algorithm work?

Key generation is easy:

▶ Primality testing (checking whether a given number is a prime or not) is computationally fast.

▶ There are many primes even among large numbers: the Prime Number Theorem says that among numbers of order $N$, on average $1$ out of $\log(N)$ numbers is a prime.

▶ So we can just start prime checking large numbers randomly, and we will soon find two primes for $p$ and $q$.

▶ $\gcd$ and $de = 1 \mod \phi(n)$ can be solved fast using the Extended Euclidean Algorithm.
RSA algorithm

Decryption and encryption are indeed inverse operations due to Euler’s Theorem:

\[ de = 1 \mod \phi(n) \implies x^{de} = x \mod n. \]
RSA algorithm

Decryption and encryption are indeed inverse operations due to Euler’s Theorem:

\[ de = 1 \mod \phi(n) \quad \implies \quad x^{de} = x \mod n. \]

Modular exponentiation (for \( x^e \) or \( c^d \)) can be computed fast along the exponents 1, 2, 4, 8, 16, \ldots
RSA algorithm

Decryption and encryption are indeed inverse operations due to Euler’s Theorem:

$$de = 1 \mod \phi(n) \implies x^{de} = x \mod n.$$ 

Modular exponentiation (for $x^e$ or $c^d$) can be computed fast along the exponents 1, 2, 4, 8, 16, …

On the other hand, integer factorization (to a product of primes) is computationally difficult for large numbers. So even though $n$ is public, $p$ and $q$ are difficult to compute, and without $p$ and $q$, we cannot compute $\phi(n)$ and $d$ either. Overall, if $p$ and $q$ are sufficiently large, attacking RSA is computationally infeasible.
RSA algorithm

Example. $p = 3, q = 11 \rightarrow n = 33$. 
RSA algorithm

Example. $p = 3, q = 11 \rightarrow n = 33$.

Then $\phi(n) = (p - 1)(q - 1) = 20$. 
Example. \( p = 3, q = 11 \rightarrow n = 33 \).

Then \( \phi(n) = (p - 1)(q - 1) = 20 \). We select \( e = 3 \). Solving

\[
d e = 1 \mod 20
\]

gives
Example. \( p = 3, q = 11 \rightarrow n = 33 \).

Then \( \phi(n) = (p - 1)(q - 1) = 20 \). We select \( e = 3 \). Solving

\[
de = 1 \mod 20
\]

gives \( d = 7 \).

Public key: \((n, e) = (20, 3)\). Private key: \( d = 7 \).

Encrypting \( x = 4 \) gives
RSA algorithm

Example. \( p = 3, q = 11 \rightarrow n = 33. \)

Then \( \phi(n) = (p - 1)(q - 1) = 20. \) We select \( e = 3. \) Solving

\[
d e = 1 \mod 20
\]

gives \( d = 7. \)

Public key: \((n, e) = (20, 3).\) Private key: \( d = 7. \)

Encrypting \( x = 4 \) gives

\[
c = x^e = 4^3 \mod 33 = 31.
\]

Decryption gives

\[
x = c^d = 31^7 = (-2)^7 = -128 = 4 \mod 33.
\]
Problem 6

The parameters of RSA are generated by \( p = 7, q = 17 \).

(a) What is the smallest possible choice of the coding exponent \( e \)?

(b) What is the cyphertext belonging to the plaintext \( x = 11 \)?

(c) What is the decoding key \( d \)?
Problem 6

The parameters of RSA are generated by $p = 7$, $q = 17$.

(a) What is the smallest possible choice of the coding exponent $e$?
(b) What is the cyphertext belonging to the plaintext $x = 11$?
(c) What is the decoding key $d$?

Solution.

(a) $\phi(n) = (p - 1)(q - 1) = 6 \cdot 16 = 96$. 

(b) $c = x^e \mod n = 11^5 \mod 119 = 160051 \mod 119 = 44$. 

(c) We need to solve $de \equiv 1 \pmod{\phi(n)}$ where $e = 5$ and $n = 96$. We use the Extended Euclidean Algorithm for $b = 96$ and $c = 5$: 

$96 = 5 \cdot 19 + 1$ 

so $d = -19 = 77 \mod 96$. 
Problem 6

The parameters of RSA are generated by $p = 7$, $q = 17$.

(a) What is the smallest possible choice of the coding exponent $e$?
(b) What is the cyphertext belonging to the plaintext $x = 11$?
(c) What is the decoding key $d$?

Solution.

(a) $\phi(n) = (p - 1)(q - 1) = 6 \cdot 16 = 96$.

We need $e$ to have $\gcd(e, 96) = 1$ and $1 < e < 96$, so the smallest possible choice for $e$ is

...
Problem 6

The parameters of RSA are generated by \( p = 7, q = 17 \).

(a) What is the smallest possible choice of the coding exponent \( e \)?

(b) What is the cyphertext belonging to the plaintext \( x = 11 \)?

(c) What is the decoding key \( d \)?

Solution.

(a) \( \phi(n) = (p - 1)(q - 1) = 6 \cdot 16 = 96 \).

We need \( e \) to have \( \gcd(e, 96) = 1 \) and \( 1 < e < 96 \), so the smallest possible choice for \( e \) is \( e = 5 \).
Problem 6

The parameters of RSA are generated by \( p = 7, q = 17 \).

(a) What is the smallest possible choice of the coding exponent \( e \)?
(b) What is the cyphertext belonging to the plaintext \( x = 11 \)?
(c) What is the decoding key \( d \)?

Solution.

(a) \( \phi(n) = (p - 1)(q - 1) = 6 \cdot 16 = 96 \).

We need \( e \) to have \( \gcd(e, 96) = 1 \) and \( 1 < e < 96 \), so the smallest possible choice for \( e \) is \( e = 5 \).

(b) \( c = x^e \mod n = 11^5 \mod 119 = 160051 \mod 119 = 44 \).
Problem 6

The parameters of RSA are generated by \( p = 7, q = 17 \).

(a) What is the smallest possible choice of the coding exponent \( e \)?
(b) What is the cyphertext belonging to the plaintext \( x = 11 \)?
(c) What is the decoding key \( d \)?

Solution.

(a) \( \phi(n) = (p - 1)(q - 1) = 6 \cdot 16 = 96 \).

We need \( e \) to have \( \gcd(e, 96) = 1 \) and \( 1 < e < 96 \), so the smallest possible choice for \( e \) is \( e = 5 \).

(b) \( c = x^e \mod n = 11^5 \mod 119 = 160051 \mod 119 = 44 \).

(c) We need to solve \( de = 1 \mod \phi(n) \) where \( e = 5 \) and \( n = 96 \).

We use the Extended Euclidean Algorithm for \( b = 96 \) and \( c = 5 \):

\[
96 = 5 \cdot 19 + 1 \quad 1 = b - 19c
\]
Problem 6

The parameters of RSA are generated by \( p = 7, q = 17 \).

(a) What is the smallest possible choice of the coding exponent \( e \)?

(b) What is the cyphertext belonging to the plaintext \( x = 11 \)?

(c) What is the decoding key \( d \)?

Solution.

(a) \( \phi(n) = (p - 1)(q - 1) = 6 \cdot 16 = 96 \).

We need \( e \) to have \( \gcd(e, 96) = 1 \) and \( 1 < e < 96 \), so the smallest possible choice for \( e \) is \( e = 5 \).

(b) \( c = x^e \mod n = 11^5 \mod 119 = 160051 \mod 119 = 44 \).

(c) We need to solve \( de = 1 \mod \phi(n) \) where \( e = 5 \) and \( n = 96 \).

We use the Extended Euclidean Algorithm for \( b = 96 \) and \( c = 5 \):

\[ 96 = 5 \cdot 19 + 1 \quad \Rightarrow \quad 1 = b - 19c \]

so \( d = -19 = 77 \mod 96 \).
Problem 6

We use RSA with $p = 73, q = 151$.

(a) Compute $n$ and $\phi(n)$.

(b) Is $e = 11$ a possible choice?

(c) Compute $d$. 

Solution.

(a) $n = 73 \cdot 151 = 11023$ and $\phi(n) = 72 \cdot 150 = 10800$.

(b) $e = 11$ is a possible choice because $\gcd(10800, 11) = 1$.

(c) Compute $d$.

$10800 = 11 \cdot 981 + 99 = 1 \cdot 10800 - 981 \cdot 11$

$11 = 9 \cdot 1 + 2 = (-1) \cdot 10800 + 982 \cdot 11$

$2 = 1 \cdot 2 + 0$.

So $d = -4909 = 5891 \mod 10800$. 

Problem 6

We use RSA with \( p = 73, q = 151 \).

(a) Compute \( n \) and \( \phi(n) \).

(b) Is \( e = 11 \) a possible choice?

(c) Compute \( d \).

Solution.

(a) \( n = 73 \cdot 151 = 11023 \) and \( \phi(n) = 72 \cdot 150 = 10800 \).

(b) \( e = 11 \) is a possible choice because \( \gcd(10800, 11) = 1 \).

(c) Compute \( d \).

\[
10800 = 11 \cdot 981 + 9 \quad \quad 9 = 1 \cdot 10800 - 981 \cdot 11
\]
Problem 6

We use RSA with \( p = 73, q = 151 \).

(a) Compute \( n \) and \( \phi(n) \).

(b) Is \( e = 11 \) a possible choice?

(c) Compute \( d \).

Solution.

(a) \( n = 73 \cdot 151 = 11023 \) and \( \phi(n) = 72 \cdot 150 = 10800 \).

(b) \( e = 11 \) is a possible choice because \( \gcd(10800, 11) = 1 \).

(c) Compute \( d \).

\[
\begin{align*}
10800 & = 11 \cdot 981 + 9 & 9 & = 1 \cdot 10800 - 981 \cdot 11 \\
11 & = 9 \cdot 1 + 2 & 2 & = (-1) \cdot 10800 + 982 \cdot 11
\end{align*}
\]
Problem 6

We use RSA with $p = 73$, $q = 151$.

(a) Compute $n$ and $\phi(n)$.
(b) Is $e = 11$ a possible choice?
(c) Compute $d$.

Solution.

(a) $n = 73 \cdot 151 = 11023$ and $\phi(n) = 72 \cdot 150 = 10800$.
(b) $e = 11$ is a possible choice because $\gcd(10800, 11) = 1$.
(c) Compute $d$.

\[
\begin{align*}
10800 &= 11 \cdot 981 + 9 & 9 &= 1 \cdot 10800 - 981 \cdot 11 \\
11 &= 9 \cdot 1 + 2 & 2 &= (-1) \cdot 10800 + 982 \cdot 11 \\
9 &= 2 \cdot 4 + 1 & 1 &= 5 \cdot 10800 - 4909 \cdot 11
\end{align*}
\]
Problem 6

We use RSA with \( p = 73, q = 151 \).

(a) Compute \( n \) and \( \phi(n) \).

(b) Is \( e = 11 \) a possible choice?

(c) Compute \( d \).

Solution.

(a) \( n = 73 \cdot 151 = 11023 \) and \( \phi(n) = 72 \cdot 150 = 10800 \).

(b) \( e = 11 \) is a possible choice because \( \gcd(10800, 11) = 1 \).

(c) Compute \( d \).

\[
\begin{align*}
10800 &= 11 \cdot 981 + 9 & 9 &= 1 \cdot 10800 - 981 \cdot 11 \\
11 &= 9 \cdot 1 + 2 & 2 &= (-1) \cdot 10800 + 982 \cdot 11 \\
9 &= 2 \cdot 4 + 1 & 1 &= 5 \cdot 10800 - 4909 \cdot 11 \\
2 &= 1 \cdot 2 + 0.
\end{align*}
\]
Problem 6

We use RSA with \( p = 73 \), \( q = 151 \).

(a) Compute \( n \) and \( \phi(n) \).

(b) Is \( e = 11 \) a possible choice?

(c) Compute \( d \).

Solution.

(a) \( n = 73 \cdot 151 = 11023 \) and \( \phi(n) = 72 \cdot 150 = 10800 \).

(b) \( e = 11 \) is a possible choice because \( \gcd(10800, 11) = 1 \).

(c) Compute \( d \).

\[
\begin{align*}
10800 &= 11 \cdot 981 + 9 & 9 &= 1 \cdot 10800 - 981 \cdot 11 \\
11 &= 9 \cdot 1 + 2 & 2 &= (-1) \cdot 10800 + 982 \cdot 11 \\
9 &= 2 \cdot 4 + 1 & 1 &= 5 \cdot 10800 - 4909 \cdot 11 \\
2 &= 1 \cdot 2 + 0.
\end{align*}
\]

So \( d = -4909 = 5891 \mod 10800 \).
Problem 7

Using the RSA code of the Problem 6, compute the cyphertext for the plaintext $x = 17$. 

Solution. We need to compute $17^{11} \mod 11023$.

\[
17^2 = 289 \mod 11023 \\
17^4 = 289^2 = 83521 = 6360 \mod 11023 \\
17^8 = 6360^2 = 40449600 = 6213 \mod 11023.
\]

$11 = 8 + 2 + 1$, so $x^{11} = x^8 \cdot x^2 \cdot x$, and we have

\[
y = 17^{11} = 6213 \cdot 289 \cdot 17 = 30524469 = 1782 \mod 11023.
\]

(In actual applications, $e = 2^{16} + 1 = 65537$ is often chosen; it is a prime, so $\gcd(n, e) > 1$ is unlikely, and $x^e = x^{2^{16}} \cdot x$ only has 2 terms.)
Problem 7

Using the RSA code of the Problem 6, compute the cyphertext for the plaintext \( x = 17 \).

Solution. We need to compute \( 17^{11} \mod 11023 \).
Problem 7

Using the RSA code of the Problem 6, compute the cyphertext for the plaintext $x = 17$.

Solution. We need to compute $17^{11} \mod 11023$.

\[
17^2 = 289 \mod 11023
\]
\[
17^4 = 289^2 = 83521 = 6360 \mod 11023
\]
\[
17^8 = 6360^2 = 40449600 = 6213 \mod 11023.
\]
Problem 7

Using the RSA code of the Problem 6, compute the cyphertext for the plaintext \( x = 17 \).

Solution. We need to compute \( 17^{11} \mod 11023 \).

\[
17^2 = 289 \mod 11023 \\
17^4 = 289^2 = 83521 = 6360 \mod 11023 \\
17^8 = 6360^2 = 40449600 = 6213 \mod 11023.
\]

\( 11 = 8 + 2 + 1 \), so \( x^{11} = x^8 \cdot x^2 \cdot x \), and we have

\[
y = 17^{11} = 6213 \cdot 289 \cdot 17 = 30524469 = 1782 \mod 11023.
\]
Problem 7

Using the RSA code of the Problem 6, compute the cyphertext for the plaintext $x = 17$.

Solution. We need to compute $17^{11} \mod 11023$.

\[
17^2 = 289 \mod 11023 \\
17^4 = 289^2 = 83521 = 6360 \mod 11023 \\
17^8 = 6360^2 = 40449600 = 6213 \mod 11023.
\]

$11 = 8 + 2 + 1$, so $x^{11} = x^8 \cdot x^2 \cdot x$, and we have

\[
y = 17^{11} = 6213 \cdot 289 \cdot 17 = 30524469 = 1782 \mod 11023.
\]

(In actual applications, $e = 2^{16} + 1 = 65537$ is often chosen; it is a prime, so $\gcd(n, e) > 1$ is unlikely, and $x^e = x^{2^{16}} \cdot x$ only has 2 terms.)