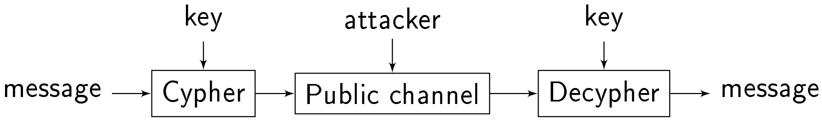
9. Cryptography

Coding Technology

Objective

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).

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!

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 $\rightarrow$ GXGTADQFA;

Problem 1

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

Solution. Guess k by trying:

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

Problem 2

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

FMXVEDKAPHFERBNDKRXRSREFMORU
DSDKDVSHVUFEDKAPRKDLYEVLRHHRH

Problem 2

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

FMXVEDKAPHFERBNDKRXRSREFMORU
DSDKDVSHVUFEDKAPRKDLYEVLRHHRH

Solution. We use statistical analysis.

English text letter probabilities

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

cyphertext letter frequencies

letter	freq.	letter	freq.
A	2	N	1
B	1	O	1
C	0	P	2
D	7	Q	0
E	5	R	8
F	4	S	3
G	0	T	0
H	5	U	2
I	0	V	4
J	0	W	0
K	5	X	2
L	2	Y	1
M	2	Z	0

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 $\to$ E, D $\to$ T. Then $E_k(4) = 17$, and $E_k(19) = 3$, that is,

$$4a + b = 17 \mod 26,$$
$$19a + b = 3 \mod 26.$$

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 $\rightarrow$ E, D $\rightarrow$ T. Then $E_k(4) = 17$, and $E_k(19) = 3$, that is,

$$4a + b = 17 \mod 26,$$
$$19a + b = 3 \mod 26.$$

Subtraction gives

$$15a = 12 \mod 26,$$

but then a must be even, so $\gcd(a, 26) > 1 \rightarrow$ incorrect guess.

Problem 2

Guess 2: R $\to$ E, E $\to$ T. Then

$$\begin{aligned} 4a + b &= 17 \mod 26, \\ 19a + b &= 4 \mod 26. \end{aligned}$$

Then

$$\begin{aligned} 15a &= 13 \mod 26, \\ a &= 13 \mod 26, \end{aligned}$$

so $\gcd(a, 26) > 1$ again $\to$ incorrect guess.

Problem 2

Guess 3: R $\to$ E, K $\to$ T. Then

$$\begin{aligned} 4a + b &= 17 \mod 26, \\ 19a + b &= 10 \mod 26. \end{aligned}$$

Then

$$\begin{aligned} 15a &= 19 \mod 26, \\ a &= 3 \mod 26, \\ b &= 5 \mod 26. \end{aligned}$$

$k = (3, 5)$ is a valid key.

Problem 2

Guess 3: R $\to$ E, K $\to$ T. Then

$$\begin{aligned} 4a + b &= 17 \mod 26, \\ 19a + b &= 10 \mod 26. \end{aligned}$$

Then

$$\begin{aligned} 15a &= 19 \mod 26, \\ a &= 3 \mod 26, \\ b &= 5 \mod 26. \end{aligned}$$

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

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

ALGORITHMSAREQUITEGENERALDEF
INITIONSOFARITHMETICPROCESSES

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.

$$\begin{matrix} 1234567 \\ 2147356 \end{matrix} \iff (12)(34765)$$

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.

$$\begin{matrix} 1234567 \\ 2147356 \end{matrix} \iff (12)(34765)$$

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:

$$\begin{array}{rcl} \text{x} & = & 01001101\ 01011101\ \ldots \\ +\text{k} & = & 11010000\ 11101011\ \ldots \\ \hline \text{y} & = & 10011101\ 10110110\ \ldots \end{array}$$

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.

Problem 3

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

Solution. $x = y + k \bmod 2$, so

$$\begin{array}{rcl} y & = & 011100010100011 \\ +k & = & 110011000001111 \\ \hline x & = & 101111010101100 \end{array}$$

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.

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.

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 $\mathrm{Pr(a)} = 1/3, \mathrm{Pr(b)} = 2/3$.
- 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:

$$\begin{array}{lll}
k = 1: & \mathrm{a}\rightarrow 1 & \mathrm{b}\rightarrow 2 \\
k = 2: & \mathrm{a}\rightarrow 2 & \mathrm{b}\rightarrow 4 \\
k = 3: & \mathrm{a}\rightarrow 3 & \mathrm{b}\rightarrow 1 \\
k = 4: & \mathrm{a}\rightarrow 5 & \mathrm{b}\rightarrow 3 \\
k = 5: & \mathrm{a}\rightarrow 4 & \mathrm{b}\rightarrow 5
\end{array}$$

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 $\Pr(\mathrm{a}) = 1/3, \Pr(\mathrm{b}) = 2/3$.
- 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:

$$
\begin{array}{lll}
k = 1: & \mathrm{a}\rightarrow 1 & \mathrm{b}\rightarrow 2 \\
k = 2: & \mathrm{a}\rightarrow 2 & \mathrm{b}\rightarrow 4 \\
k = 3: & \mathrm{a}\rightarrow 3 & \mathrm{b}\rightarrow 1 \\
k = 4: & \mathrm{a}\rightarrow 5 & \mathrm{b}\rightarrow 3 \\
k = 5: & \mathrm{a}\rightarrow 4 & \mathrm{b}\rightarrow 5
\end{array}
$$

(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:

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

Problem 5 – stochastic encryption

Solution.

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

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

(b) No, e.g.

$$\Pr(Y=1|X=\text{a}) = 2/5 \neq \Pr(Y=1|X=\text{b}) = 1/5.$$

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

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

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

$$s_{k+1} = s_{k-1} - q_k s_k, \qquad t_{k+1} = t_{k-1} - q_k t_k.$$

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

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

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

$$s_{k+1} = s_{k-1} - q_k s_k, \qquad t_{k+1} = t_{k-1} - q_k t_k.$$

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

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

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

$$s_{k+1} = s_{k-1} - q_k s_k, \qquad t_{k+1} = t_{k-1} - q_k t_k.$$

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 $e^{-1} = t \bmod n$.

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 (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.

$$8387 = 1243 \cdot 6 + 929 \qquad 929 = b - 6c$$

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.

$$\begin{aligned} 8387 &= 1243 \cdot 6 + 929 \qquad & 929 &= b - 6c \\ 1243 &= 929 \cdot 1 + 314 \qquad & 314 &= -b + 7c \end{aligned}$$

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.

$$\begin{aligned} 8387 &= 1243 \cdot 6 + 929 & \qquad 929 &= b - 6c \\ 1243 &= 929 \cdot 1 + 314 & \qquad 314 &= -b + 7c \\ 929 &= 314 \cdot 2 + 301 & \qquad 301 &= 3b - 20c \end{aligned}$$

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.

$$\begin{aligned} 8387 &= 1243 \cdot 6 + 929 \qquad & 929 &= b - 6c \\ 1243 &= 929 \cdot 1 + 314 & 314 &= -b + 7c \\ 929 &= 314 \cdot 2 + 301 & 301 &= 3b - 20c \\ 314 &= 301 \cdot 1 + 13 & 13 &= -4b + 27c \end{aligned}$$

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.

$$\begin{aligned} 8387 &= 1243 \cdot 6 + 929 & 929 &= b - 6c \\ 1243 &= 929 \cdot 1 + 314 & 314 &= -b + 7c \\ 929 &= 314 \cdot 2 + 301 & 301 &= 3b - 20c \\ 314 &= 301 \cdot 1 + 13 & 13 &= -4b + 27c \\ 301 &= 13 \cdot 23 + 2 & 2 &= 95b - 641c \end{aligned}$$

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.

$$\begin{aligned}
8387 &= 1243 \cdot 6 + 929 & \qquad 929 &= b - 6c \\
1243 &= 929 \cdot 1 + 314 & 314 &= -b + 7c \\
929 &= 314 \cdot 2 + 301 & 301 &= 3b - 20c \\
314 &= 301 \cdot 1 + 13 & 13 &= -4b + 27c \\
301 &= 13 \cdot 23 + 2 & 2 &= 95b - 641c \\
13 &= 2 \cdot 6 + 1 & 1 &= -574b + 3873c
\end{aligned}$$

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.

$$\begin{aligned} 8387 &= 1243 \cdot 6 + 929 \\ 1243 &= 929 \cdot 1 + 314 \\ 929 &= 314 \cdot 2 + 301 \\ 314 &= 301 \cdot 1 + 13 \\ 301 &= 13 \cdot 23 + 2 \\ 13 &= 2 \cdot 6 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned} \qquad \begin{aligned} 929 &= b - 6c \\ 314 &= -b + 7c \\ 301 &= 3b - 20c \\ 13 &= -4b + 27c \\ 2 &= 95b - 641c \\ 1 &= -574b + 3873c \end{aligned}$$

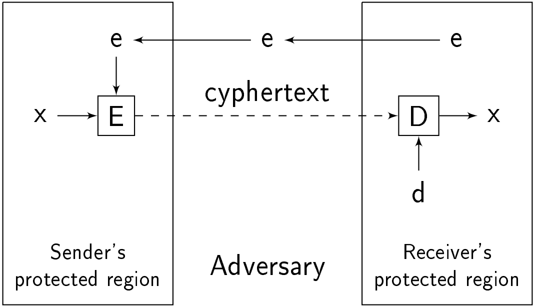
Finally,

$$\gcd(8387, 1243) = -574 \cdot 8387 + 3873 \cdot 1243.$$

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.

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 $c = x^e \mod n$.

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:
  - $x = c^d \mod n$.

RSA algorithm

Why does the RSA algorithm work?

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:

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

RSA algorithm

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

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

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:

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

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

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. $p = 3, q = 11 \to n = 33.$

RSA algorithm

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

Then $\phi(n) = (p-1)(q-1) = 20.$

RSA algorithm

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

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

$$de = 1 \mod 20$$

gives

RSA algorithm

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

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. $p = 3, q = 11 \to n = 33$.

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

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

Decryption gives

$$x = c^d = 31^7 = (-2)^7 = -128 = 4 \bmod 33.$$

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

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) $c = x^e \bmod n = 11^5 \bmod 119 = 160051 \bmod 119 = 44$.

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) $c = x^e \bmod n = 11^5 \bmod 119 = 160051 \bmod 119 = 44$.

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

$$96 = 5 \cdot 19 + 1 \qquad 1 = b - 19c$$

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) $c = x^e \bmod n = 11^5 \bmod 119 = 160051 \bmod 119 = 44.$

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

$$96 = 5 \cdot 19 + 1 \qquad 1 = b - 19c$$

so $d = -19 = 77 \bmod 96$.

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.

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.

$$10800 = 11 \cdot 981 + 9 \qquad 9 = 1 \cdot 10800 - 981 \cdot 11$$

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.

$$\begin{aligned} 10800 &= 11 \cdot 981 + 9 \qquad & 9 &= 1 \cdot 10800 - 981 \cdot 11 \\ 11 &= 9 \cdot 1 + 2 \qquad & 2 &= (-1) \cdot 10800 + 982 \cdot 11 \end{aligned}$$

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.

$$\begin{aligned} 10800 &= 11 \cdot 981 + 9 & \qquad 9 &= 1 \cdot 10800 - 981 \cdot 11 \\ 11 &= 9 \cdot 1 + 2 & 2 &= (-1) \cdot 10800 + 982 \cdot 11 \\ 9 &= 2 \cdot 4 + 1 & 1 &= 5 \cdot 10800 - 4909 \cdot 11 \end{aligned}$$

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.

$$\begin{aligned} 10800 &= 11 \cdot 981 + 9 \\ 11 &= 9 \cdot 1 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned} \qquad \begin{aligned} 9 &= 1 \cdot 10800 - 981 \cdot 11 \\ 2 &= (-1) \cdot 10800 + 982 \cdot 11 \\ 1 &= 5 \cdot 10800 - 4909 \cdot 11 \end{aligned}$$

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.

$$\begin{aligned} 10800 &= 11 \cdot 981 + 9 \\ 11 &= 9 \cdot 1 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned} \qquad \begin{aligned} 9 &= 1 \cdot 10800 - 981 \cdot 11 \\ 2 &= (-1) \cdot 10800 + 982 \cdot 11 \\ 1 &= 5 \cdot 10800 - 4909 \cdot 11 \end{aligned}$$

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

Problem 7

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

Problem 7

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

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

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.)