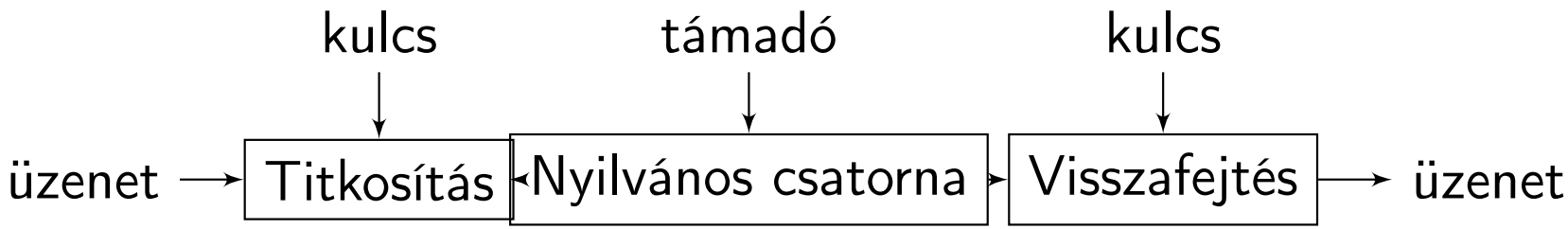
9. Titkosítás

Kódolástechnika

Motiváció

A cél: biztonságos titkos kommunikáció nyilvános csatornán keresztül.



Szeretnénk olyan titkosító eljárásokat tervezni, amelyek a támadó számára nagy komplexitású feladatot jelentenek, de a kulcs ismeretében a titkosított üzenet könnyen visszafejthető.

Egyszerű titkosítások I

Additív titkosítás. Ha az ábécé mérete n (pl. az angol ábécére $n = 26$), akkor

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

ahol k a kulcs értéke, x az üzenet (nyílt szöveg), y pedig a titkosított szöveg.
Ha k ismeretlen, akkor találgatással lehet próbálkozni (pl. az angol ábécé esetén 26 lehetőség van).

Egyszerű titkosítások I

Additív titkosítás. Ha az ábécé mérete n (pl. az angol ábécére $n = 26$), akkor

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

ahol k a kulcs értéke, x az üzenet (nyílt szöveg), y pedig a titkosított szöveg.
Ha k ismeretlen, akkor találgatással lehet próbálkozni (pl. az angol ábécé esetén 26 lehetőség van).

Lineáris titkosítás:

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

ahol $k = (a, b)$ a kulcs értéke. $\gcd(a, n) = 1$-nek teljesülnie kell!

Egyszerű titkosítások I

Additív titkosítás. Ha az ábécé mérete n (pl. az angol ábécére $n = 26$), akkor

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

ahol k a kulcs értéke, x az üzenet (nyílt szöveg), y pedig a titkosított szöveg.
Ha k ismeretlen, akkor találgatással lehet próbálkozni (pl. az angol ábécé esetén 26 lehetőség van).

Lineáris titkosítás:

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

ahol $k = (a, b)$ a kulcs értéke. $\gcd(a, n) = 1$-nek teljesülnie kell! A visszafejtés is lineáris:

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

Ismeretlen kulcs esetén statisztikus analízis segíthet a találgatásban.

1. feladat

Fejtsük vissza a HYHUBERGB titkosított szöveget, ha tudjuk, hogy $y = x + k \mod 26$ alakú additív titkosítással kódolták.

1. feladat

Fejtsük vissza a HYHUBERGB titkosított szöveget, ha tudjuk, hogy $y = x + k \mod 26$ alakú additív titkosítással kódolták.

Megoldás. Tippelünk k értékére:

- $k = 1$: HYHUBERGB $\rightarrow$ GXGTADQFA;

1. feladat

Fejtsük vissza a HYHUBERGB titkosított szöveget, ha tudjuk, hogy $y = x + k \mod 26$ alakú additív titkosítással kódolták.

Megoldás. Tippelünk k értékére:

- $k = 1$: HYHUBERGB $\to$ GXGTADQFA;
- $k = 2$: HYHUBERGB $\to$ FWFSZCPEZ;

1. feladat

Fejtsük vissza a HYHUBERGB titkosított szöveget, ha tudjuk, hogy $y = x + k \mod 26$ alakú additív titkosítással kódolták.

Megoldás. Tippelünk k értékére:

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

2. feladat

Fejtsük vissza a következő titkosított szöveget, ha tudjuk, hogy lineáris titkosítással kódolták.

FMXVEDKAPHFERBNDKRXRSREFMORU
DSDKDVSHVUFEDKAPRKDLYEVLRHHRH

2. feladat

Fejtsük vissza a következő titkosított szöveget, ha tudjuk, hogy lineáris titkosítással kódolták.

FMXVEDKAPHFERBNDKRXRSREFMORU
DSDKDVSHVUFEDKAPRKDLYEVLRHHRH

Megoldás. Statisztikus analízist használunk.

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

a titkosított szövegbeli előfordulások

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

2. feladat

A titkosított szövegben a leggyakoribb betűk: R(8), D(7), E(5), H(5), K(5).

Ezek jó jelöltek E-re és T-re (a két leggyakoribb betű az angol ábécében).

2. feladat

A titkosított szövegben a leggyakoribb betűk: R(8), D(7), E(5), H(5), K(5).

Ezek jó jelöltek E-re és T-re (a két leggyakoribb betű az angol ábécében).

1. tipp: R $\to$ E, D $\to$ T. Ekkor $E_k(4) = 17$, és $E_k(19) = 3$, ahonnan

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

2. feladat

A titkosított szövegben a leggyakoribb betűk: R(8), D(7), E(5), H(5), K(5).

Ezek jó jelöltek E-re és T-re (a két leggyakoribb betű az angol ábécében).

1. tipp: R $\to$ E, D $\to$ T. Ekkor $E_k(4) = 17$, és $E_k(19) = 3$, ahonnan

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

Kivonva a két egyeneletet

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

ám ekkor a értéke páros lesz, így $\gcd(a, 26) > 1 \to$ rossz volt a tipp.

2. feladat

2. tipp: R $\to$ E, E $\to$ T. Ekkor

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

és

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

így ismét csak $\gcd(a, 26) > 1 \to$ ez a tipp is rossz volt.

2. feladat

3. tipp: R $\to$ E, H $\to$ T. Ekkor

$$4a + b = 17 \mod 26,$$
$$19a + b = 7 \mod 26,$$

ahonnan

$$15a = 10 \mod 26,$$

tehát a ismét páros $\to$ ez a tipp is rossz volt.

2. feladat

4. tipp: R $\to$ E, K $\to$ T. Ekkor

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

Innen

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

$k = (3, 5)$ jó kulcs.

2. feladat

4. tipp: R $\to$ E, K $\to$ T. Ekkor

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

Innen

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

$k = (3, 5)$ jó kulcs. Még ellenőriznünk kell, hogy a visszafejtett szöveg értelmes-e.

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

ALGORITHMSAREQUITEGENERALDEF
INITIONSOFARITHMETICPROCESSES

Egyszerű titkosítások II

Permutációs titkosítás: az üzeneteket egyforma hosszú szakaszokra vágjuk, majd minden szakaszon belül a karaktereket egy rögzített permutációnak megfelelően összekeverjük.

Példa.

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

Titkosítás: MORNING $\rightarrow$ OMIRNGN

Egyszerű titkosítások II

Permutációs titkosítás: az üzeneteket egyforma hosszú szakaszokra vágjuk, majd minden szakaszon belül a karaktereket egy rögzített permutációnak megfelelően összekeverjük.

Példa.

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

Titkosítás: MORNING $\rightarrow$ OMIRNGN

Egyszer használatos kulcs (One time pad, OTP): a küldő és vevő rendelkezésére áll ugyanaz a titkos, véletlenszerű k bitsorozat; a titkosítás az üzenet és a kulcs bitenkénti összeadása. Példa:

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

Amíg a kulcsot csak egyszer használjuk, az OTP tökéletes titkosságot garantál. (És egyébként ez lényegében az egyetlen ilyen titkosítás.)

3. feladat

Egy üzenetet OTP használatával titkosítottak, a kulcs
$k = (110011000001111)$, a titkosított szöveg
$y = (011100010100011)$. Adjuk meg az eredeti x nyílt szöveget.

3. feladat

Egy üzenetet OTP használatával titkosítottak, a kulcs $k = (110011000001111)$, a titkosított szöveg $y = (011100010100011)$. Adjuk meg az eredeti x nyílt szöveget.

Megoldás. $x = y + k \bmod 2$, tehát

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

4. feladat – OTP közös kulcs nélkül

A és B úgy akarnak kommunikálni, hogy OTP-t használnak közös kulcs nélkül. Legyen A kulcsa k_A, B kulcsa pedig k_B. A átküldi az $y_1 = x + k_A$ szöveget B-nek, aki erre visszaküldi az $y_2 = y_1 + k_B$ szöveget, végül A az $y_3 = y_2 + k_A$ szöveget küldi vissza. Az

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

értékekből számítsuk ki az x nyílt szöveget és a k_A és k_B kulcsokat.

4. feladat – OTP közös kulcs nélkül

A és B úgy akarnak kommunikálni, hogy OTP-t használnak közös kulcs nélkül. Legyen A kulcsa k_A, B kulcsa pedig k_B. A átküldi az $y_1 = x + k_A$ szöveget B-nek, aki erre visszaküldi az $y_2 = y_1 + k_B$ szöveget, végül A az $y_3 = y_2 + k_A$ szöveget küldi vissza. Az

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

értékekből számítsuk ki az x nyílt szöveget és a k_A és k_B kulcsokat.

Megoldás.

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

4. feladat – OTP közös kulcs nélkül

A és B úgy akarnak kommunikálni, hogy OTP-t használnak közös kulcs nélkül. Legyen A kulcsa k_A, B kulcsa pedig k_B. A átküldi az $y_1 = x + k_A$ szöveget B-nek, aki erre visszaküldi az $y_2 = y_1 + k_B$ szöveget, végül A az $y_3 = y_2 + k_A$ szöveget küldi vissza. Az

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

értékekből számítsuk ki az x nyílt szöveget és a k_A és k_B kulcsokat.

Megoldás.

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

Innen

$$x = y_1 + y_2 + y_3 = (0111011011),$$
$$k_A = x + y_1 = (0000011111),$$
$$k_B = x + y_3 = (1111100000).$$

5. feladat – sztochasztikus titkosítás

Sztochasztikus titkosításnál a k kulcsot véletlenszerűen választjuk.

5. feladat – sztochasztikus titkosítás

Sztochasztikus titkosításnál a k kulcsot véletlenszerűen választjuk.
Tekintsük a következő rendszert:

- a nyílt szövegek ábécéje {a,b}, a valószínűségeik $\Pr(a) = 1/3, \Pr(b) = 2/3$.
- a titkosított szövegek ábécéje {1,2,3,4,5}.
- a kulcsok {1,2,3,4,5}, melyeket rendre $\{2/5, 1/5, 1/5, 1/10, 1/10\}$ valószínűséggel választunk.

5. feladat – sztochasztikus titkosítás

Sztochasztikus titkosításnál a k kulcsot véletlenszerűen választjuk.
Tekintsük a következő rendszert:

- a nyílt szövegek ábécéje {a,b}, a valószínűségeik $\Pr(a) = 1/3, \Pr(b) = 2/3$.
- a titkosított szövegek ábécéje {1,2,3,4,5}.
- a kulcsok {1,2,3,4,5}, melyeket rendre $\{2/5, 1/5, 1/5, 1/10, 1/10\}$ valószínűséggel választunk.

A nyílt szöveg $\rightarrow$ titkosított szöveg hozzárendelés a következő:

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

5. feladat – sztochasztikus titkosítás

Sztochasztikus titkosításnál a k kulcsot véletlenszerűen választjuk. Tekintsük a következő rendszert:

- a nyílt szövegek ábécéje {a,b}, a valószínűségeik $\Pr(a) = 1/3, \Pr(b) = 2/3$.
- a titkosított szövegek ábécéje {1,2,3,4,5}.
- a kulcsok {1,2,3,4,5}, melyeket rendre $\{2/5, 1/5, 1/5, 1/10, 1/10\}$ valószínűséggel választunk.

A nyílt szöveg $\rightarrow$ titkosított szöveg hozzárendelés a következő:

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

(a) Számítsuk ki a titkosított ábécé eloszlását.

(b) A nyílt szöveg és a titkosított szöveg független-e (vagyis ez egy tökéletes titkosítás)?

5. feladat – sztochasztikus titkosítás

Megoldás.

(a) Teljes valószínűség tétele alapján:

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

5. feladat – sztochasztikus titkosítás

Megoldás.

(a) Teljes valószínűség tétele alapján:

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

(b) Nem, pl.

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

Kiterjesztett Euklideszi Algoritmus

A Kiterjesztett Euklideszi Algoritmussal kiszámítható $\gcd(a, b)$ értéke (legnagyobb közös osztó), továbbá olyan s, t is, melyekre

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

Kiterjesztett Euklideszi Algoritmus

A Kiterjesztett Euklideszi Algoritmussal kiszámítható $\gcd(a, b)$ értéke (legnagyobb közös osztó), továbbá olyan s, t is, melyekre

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

Legyen $a > b$; kezdetben $r_0 = a, r_1 = b$ és $s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1$. Minden egyes lépésben felírjuk az

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

egyenleteket, ahol $0 \leq r_{k+1} < r_k$, és s_{k+1} és t_{k_+1} értékére a képlet

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

Kiterjesztett Euklideszi Algoritmus

A Kiterjesztett Euklideszi Algoritmussal kiszámítható $\gcd(a, b)$ értéke (legnagyobb közös osztó), továbbá olyan s, t is, melyekre

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

Legyen $a > b$; kezdetben $r_0 = a, r_1 = b$ és $s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1$. Minden egyes lépésben felírjuk az

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

egyenleteket, ahol $0 \leq r_{k+1} < r_k$, és s_{k+1} és t_{k_+1} értékére a képlet

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

Az algoritmus megáll, amikor $r_{k+1} = 0$; ekkor $r_k = \gcd(a, b)$, és $\gcd(a, b) = s_k \cdot a + t_k \cdot b$. Ismert, hogy tetszőleges a, b-re legfeljebb $\log_{1.62}(\min(a, b))$ lépésre van szükség.

Kiterjesztett Euklideszi Algoritmus

A Kiterjesztett Euklideszi Algoritmussal kiszámítható $\gcd(a, b)$ értéke (legnagyobb közös osztó), továbbá olyan s, t is, melyekre

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

Legyen $a > b$; kezdetben $r_0 = a, r_1 = b$ és $s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1$. Minden egyes lépésben felírjuk az

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

egyenleteket, ahol $0 \leq r_{k+1} < r_k$, és s_{k+1} és t_{k_1} értékére a képlet

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

Az algoritmus megáll, amikor $r_{k+1} = 0$; ekkor $r_k = \gcd(a, b)$, és $\gcd(a, b) = s_k \cdot a + t_k \cdot b$. Ismert, hogy tetszőleges a, b-re legfeljebb $\log_{1.62}(\min(a, b))$ lépésre van szükség.

Ha $\gcd(n, e) = 1$, akkor $1 = \gcd(n, e) = s \cdot n + t \cdot e$, vagyis $e^{-1} = t \mod n$.

5. feladat

Számítsuk ki $a = 8387$ és $b = 1243$ legnagyobb közös osztóját (gcd), valamint adjunk meg olyan s és t értékeket, hogy

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

5. feladat

Számítsuk ki $a = 8387$ és $b = 1243$ legnagyobb közös osztóját (gcd), valamint adjunk meg olyan s és t értékeket, hogy

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

Megoldás.

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

5. feladat

Számítsuk ki $a = 8387$ és $b = 1243$ legnagyobb közös osztóját (gcd), valamint adjunk meg olyan s és t értékeket, hogy

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

Megoldás.

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

5. feladat

Számítsuk ki $a = 8387$ és $b = 1243$ legnagyobb közös osztóját (gcd), valamint adjunk meg olyan s és t értékeket, hogy

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

Megoldás.

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

5. feladat

Számítsuk ki $a = 8387$ és $b = 1243$ legnagyobb közös osztóját (gcd), valamint adjunk meg olyan s és t értékeket, hogy

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

Megoldás.

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

5. feladat

Számítsuk ki $a = 8387$ és $b = 1243$ legnagyobb közös osztóját (gcd), valamint adjunk meg olyan s és t értékeket, hogy

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

Megoldás.

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

5. feladat

Számítsuk ki $a = 8387$ és $b = 1243$ legnagyobb közös osztóját (gcd), valamint adjunk meg olyan s és t értékeket, hogy

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

Megoldás.

$$\begin{aligned}
8387 &= 1243 \cdot 6 + 929 \\
1243 &= 929 \cdot 1 + 314 \\
929 &= 314 \cdot 2 + 301 \\
314 &= 301 \cdot 1 + 13 \\
301 &= 13 \cdot 23 + 2 \\
13 &= 2 \cdot 6 + 1
\end{aligned}$$

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

5. feladat

Számítsuk ki $a = 8387$ és $b = 1243$ legnagyobb közös osztóját (gcd), valamint adjunk meg olyan s és t értékeket, hogy

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

Megoldás.

$$\begin{aligned}
8387 &= 1243 \cdot 6 + 929 \\
1243 &= 929 \cdot 1 + 314 \\
929 &= 314 \cdot 2 + 301 \\
314 &= 301 \cdot 1 + 13 \\
301 &= 13 \cdot 23 + 2 \\
13 &= 2 \cdot 6 + 1 \\
2 &= 1 \cdot 2 + 0.
\end{aligned}$$

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

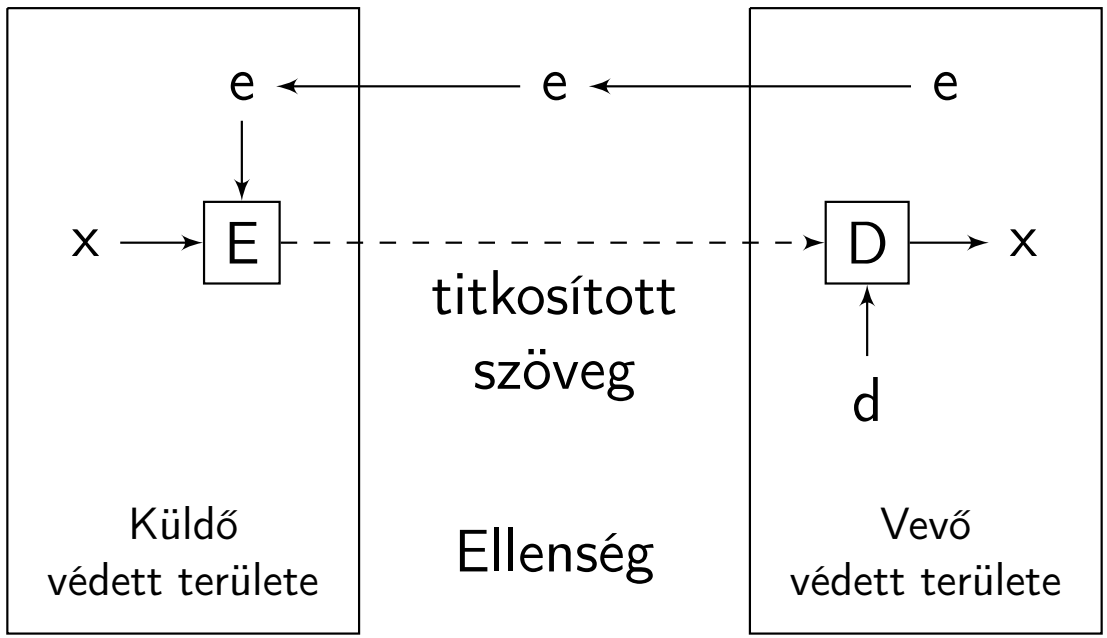
Finally,

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

Nyilvános kulcsú titkosítás

A nyilvános kulcsú titkosítás esetében nincs egy közös k kulcs, amelyet a küldő és a vevő is ismer, hanem:

- a vevőnek van egy (d, e) kulcspárja;
- d egy titkos kulcs, amelyet csak a vevő ismer;
- e egy nyilvános kulcs, amelyet mindenki ismer



RSA algoritmus

Az RSA algoritmus a következő lépésekből áll:

- Kulcs generálás:
  - választunk 2 nagy p és q prímszámot; $n = pq$.
  - $\phi(n) = (p-1)(q-1)$.
  - Választunk egy e kódoló exponenst úgy, hogy $\gcd(e, \phi(n)) = 1$ és $1 < e < \phi(n)$.
  - A $de = 1 \bmod \phi(n)$ egyenlet megoldása a d dekódoló kulcs.
  - (n, e) a nyilvános kulcs;
  - $p, q, \phi(n)$ és d titkosak.

RSA algoritmus

Az RSA algoritmus a következő lépésekből áll:

- Kulcs generálás:
  - választunk 2 nagy p és q prímszámot; $n = pq$.
  - $\phi(n) = (p-1)(q-1)$.
  - Választunk egy e kódoló exponenst úgy, hogy $\gcd(e, \phi(n)) = 1$ és $1 < e < \phi(n)$.
  - A $de = 1 \bmod \phi(n)$ egyenlet megoldása a d dekódoló kulcs.
  - (n, e) a nyilvános kulcs;
  - $p, q, \phi(n)$ és d titkosak.
- Titkosítás (a nyilvános kulcs használatával):
  - a nyílt szöveget felvágjuk olyan szakaszokra, melyek megfeleltethetőek egy-egy x számnak, melyre $0 \leq x < n$.
  - a titkosított szöveg $c = x^e \mod n$.

RSA algoritmus

Az RSA algoritmus a következő lépésekből áll:

- Kulcs generálás:
  - választunk 2 nagy p és q prímszámot; $n = pq$.
  - $\phi(n) = (p-1)(q-1)$.
  - Választunk egy e kódoló exponenst úgy, hogy $\gcd(e, \phi(n)) = 1$ és $1 < e < \phi(n)$.
  - A $de = 1 \bmod \phi(n)$ egyenlet megoldása a d dekódoló kulcs.
  - (n, e) a nyilvános kulcs;
  - $p, q, \phi(n)$ és d titkosak.
- Titkosítás (a nyilvános kulcs használatával):
  - a nyílt szöveget felvágjuk olyan szakaszokra, melyek megfeleltethetőek egy-egy x számnak, melyre $0 \leq x < n$.
  - a titkosított szöveg $c = x^e \mod n$.
- Visszafejtés:
  - $x = c^d \mod n$.

RSA algoritmus

Miért jó az RSA algoritms?

RSA algoritmus

Miért jó az RSA algoritms?

Kulcsot lehet gyorsan generálni:

- A prímtesztelésre (tehát annak eldöntésére, hogy egy egész szám prímszám-e) ismertek gyors eljárások.
- A prímszámok viszonylag sűrűn vannak: a Prímszámtétel szerint aszimptotikusan az N nagyságrendű számok között átlagosan minden $\log(N)$-edik szám prímszám.
- Tehát elkezdhetünk nagy számokat találomra prímtesztelni, és előbb-utóbb találunk két prímszámot p-nek és q-nak.
- gcd és $de = 1 \bmod \phi(n)$ gyorsan kiszámíthatóak a Kiterjesztett Euklideszi Algoritmussal.

RSA algoritmus

A titkosítás és a visszafejtés tényleg inverz operációk az Euler-tétel miatt:

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

RSA algoritmus

A titkosítás és a visszafejtés tényleg inverz operációk az Euler-tétel miatt:

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

A mod n hatványozás (x^e és c^d kiszámításához) gyorsan kiszámítható az $1, 2, 4, 8, 16, \ldots$ kitevők mentén.

RSA algoritmus

A titkosítás és a visszafejtés tényleg inverz operációk az Euler-tétel miatt:

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

A mod n hatványozás (x^e és c^d kiszámításához) gyorsan kiszámítható az $1, 2, 4, 8, 16, \ldots$ kitevők mentén.

Másrészt viszont a prímtényezőkre bontásra nem ismert gyors algoritmus nagy számokra. Tehát annak ellenére, hogy n nyilvános, p és q a gyakorlatban mégsem kiszámítható n ismeretében, és p és q nélkül $\phi(n)$ és d sem kiszámítható. Összességében ha p és q kellően nagy, akkor az RSA titkosítás nem támadható hatékonyan.

RSA algoritmus

Példa. $p = 3, q = 11 \to n = 33$.

RSA algoritmus

Példa. $p = 3, q = 11 \to n = 33$.

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

RSA algoritmus

Példa. $p = 3, q = 11 \to n = 33$.

Ekkor $\phi(n) = (p-1)(q-1) = 20$. Legyen $e = 3$.

$$de = 1 \mod 20$$

megoldása

RSA algoritmus

Példa. $p = 3, q = 11 \to n = 33$.

Ekkor $\phi(n) = (p-1)(q-1) = 20$. Legyen $e = 3$.

$$de = 1 \mod 20$$

megoldása $d = 7$.

Nyilvános kulcs: $(n, e) = (20, 3)$. Titkos kulcs: $d = 7$.

$x = 4$ titkosítva

RSA algoritmus

Példa. $p = 3, q = 11 \to n = 33$.

Ekkor $\phi(n) = (p-1)(q-1) = 20$. Legyen $e = 3$.

$$de = 1 \mod 20$$

megoldása $d = 7$.

Nyilvános kulcs: $(n, e) = (20, 3)$. Titkos kulcs: $d = 7$.

$x = 4$ titkosítva

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

A visszafejtés pedig

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

6. feladat

A $p = 7, q = 17$ prímekből kiindulva készítünk RSA titkosítást.

(a) Mi az e kódoló exponens lehetséges legkisebb értéke?

(b) Mi az $x = 11$ nyílt szöveghez tartozó titkosított szöveg?

(c) Mi a d visszafejtő kulcs?

6. feladat

A $p = 7, q = 17$ prímekből kiindulva készítünk RSA titkosítást.

(a) Mi az e kódoló exponens lehetséges legkisebb értéke?

(b) Mi az $x = 11$ nyílt szöveghez tartozó titkosított szöveg?

(c) Mi a d visszafejtő kulcs?

Megoldás.

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

6. feladat

A $p = 7, q = 17$ prímekből kiindulva készítünk RSA titkosítást.

(a) Mi az e kódoló exponens lehetséges legkisebb értéke?

(b) Mi az $x = 11$ nyílt szöveghez tartozó titkosított szöveg?

(c) Mi a d visszafejtő kulcs?

Megoldás.

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

Teljesülnie kell, hogy $\gcd(e, 96) = 1$ és $1 < e < 96$, így a legkisebb megfelelő e érték

6. feladat

A $p = 7, q = 17$ prímekből kiindulva készítünk RSA titkosítást.

(a) Mi az e kódoló exponens lehetséges legkisebb értéke?

(b) Mi az $x = 11$ nyílt szöveghez tartozó titkosított szöveg?

(c) Mi a d visszafejtő kulcs?

Megoldás.

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

Teljesülnie kell, hogy $\gcd(e, 96) = 1$ és $1 < e < 96$, így a legkisebb megfelelő e érték az $e = 5$.

6. feladat

A $p = 7, q = 17$ prímekből kiindulva készítünk RSA titkosítást.

(a) Mi az e kódoló exponens lehetséges legkisebb értéke?

(b) Mi az $x = 11$ nyílt szöveghez tartozó titkosított szöveg?

(c) Mi a d visszafejtő kulcs?

Megoldás.

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

Teljesülnie kell, hogy $\gcd(e, 96) = 1$ és $1 < e < 96$, így a legkisebb megfelelő e érték az $e = 5$.

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

6. feladat

A $p = 7, q = 17$ prímekből kiindulva készítünk RSA titkosítást.

(a) Mi az e kódoló exponens lehetséges legkisebb értéke?

(b) Mi az $x = 11$ nyílt szöveghez tartozó titkosított szöveg?

(c) Mi a d visszafejtő kulcs?

Megoldás.

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

Teljesülnie kell, hogy $\gcd(e, 96) = 1$ és $1 < e < 96$, így a legkisebb megfelelő e érték az $e = 5$.

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

(c) Meg kell oldanunk a $de = 1 \bmod \phi(n)$ egyenletet, ahol $e = 5$ és $\phi(n) = 96$. A Kiterjesztett Euklideszi Algoritmust használjuk:

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

6. feladat

A $p = 7, q = 17$ prímekből kiindulva készítünk RSA titkosítást.

(a) Mi az e kódoló exponens lehetséges legkisebb értéke?

(b) Mi az $x = 11$ nyílt szöveghez tartozó titkosított szöveg?

(c) Mi a d visszafejtő kulcs?

Megoldás.

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

Teljesülnie kell, hogy $\gcd(e, 96) = 1$ és $1 < e < 96$, így a legkisebb megfelelő e érték az $e = 5$.

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

(c) Meg kell oldanunk a $de = 1 \bmod \phi(n)$ egyenletet, ahol $e = 5$ és $\phi(n) = 96$. A Kiterjesztett Euklideszi Algoritmust használjuk:

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

tehát $d = -19 = 77 \bmod 96$.

7. feladat

A $p = 73, q = 151$ prímekből kiindulva készítünk RSA titkosítást.

(a) Számítsuk ki n és $\phi(n)$ értékét.

(b) $e = 11$ lehetséges választás-e?

(c) Adjuk meg d értékét.

7. feladat

A $p = 73, q = 151$ prímekből kiindulva készítünk RSA titkosítást.

(a) Számítsuk ki n és $\phi(n)$ értékét.

(b) $e = 11$ lehetséges választás-e?

(c) Adjuk meg d értékét.

Megoldás.

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

(b) $e = 11$ lehetséges választás, mivel $\gcd(10800, 11) = 1$.

(c) Kiszámítjuk d-t.

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

7. feladat

A $p = 73, q = 151$ prímekből kiindulva készítünk RSA titkosítást.

(a) Számítsuk ki n és $\phi(n)$ értékét.

(b) $e = 11$ lehetséges választás-e?

(c) Adjuk meg d értékét.

Megoldás.

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

(b) $e = 11$ lehetséges választás, mivel $\gcd(10800, 11) = 1$.

(c) Kiszámítjuk d-t.

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

7. feladat

A $p = 73, q = 151$ prímekből kiindulva készítünk RSA titkosítást.

(a) Számítsuk ki n és $\phi(n)$ értékét.

(b) $e = 11$ lehetséges választás-e?

(c) Adjuk meg d értékét.

Megoldás.

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

(b) $e = 11$ lehetséges választás, mivel $\gcd(10800, 11) = 1$.

(c) Kiszámítjuk d-t.

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

7. feladat

A $p = 73, q = 151$ prímekből kiindulva készítünk RSA titkosítást.

(a) Számítsuk ki n és $\phi(n)$ értékét.

(b) $e = 11$ lehetséges választás-e?

(c) Adjuk meg d értékét.

Megoldás.

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

(b) $e = 11$ lehetséges választás, mivel $\gcd(10800, 11) = 1$.

(c) Kiszámítjuk d-t.

$$\begin{aligned} 10800 &= 11 \cdot 981 + 9 \\ 11 &= 9 \cdot 1 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

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

7. feladat

A $p = 73, q = 151$ prímekből kiindulva készítünk RSA titkosítást.

(a) Számítsuk ki n és $\phi(n)$ értékét.

(b) $e = 11$ lehetséges választás-e?

(c) Adjuk meg d értékét.

Megoldás.

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

(b) $e = 11$ lehetséges választás, mivel $\gcd(10800, 11) = 1$.

(c) Kiszámítjuk d-t.

$$\begin{aligned} 10800 &= 11 \cdot 981 + 9 \\ 11 &= 9 \cdot 1 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

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

Tehát $d = -4909 = 5891 \bmod 10800$.

8. feladat

Az előző feladat titkosításával titkosítsuk az $x = 17$ nyílt szöveget.

8. feladat

Az előző feladat titkosításával titkosítsuk az $x = 17$ nyílt szöveget.

Megoldás. Ki kell számítanunk $17^{11} \bmod 11023$ értékét.

8. feladat

Az előző feladat titkosításával titkosítsuk az $x = 17$ nyílt szöveget.

Megoldás. Ki kell számítanunk $17^{11} \bmod 11023$ értékét.

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

8. feladat

Az előző feladat titkosításával titkosítsuk az $x = 17$ nyílt szöveget.

Megoldás. Ki kell számítanunk $17^{11} \bmod 11023$ értékét.

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

$11 = 8 + 2 + 1$, tehát $x^{11} = x^8 \cdot x^2 \cdot x$, ahonnan

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

8. feladat

Az előző feladat titkosításával titkosítsuk az $x = 17$ nyílt szöveget.

Megoldás. Ki kell számítanunk $17^{11} \bmod 11023$ értékét.

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

$11 = 8 + 2 + 1$, tehát $x^{11} = x^8 \cdot x^2 \cdot x$, ahonnan

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

(A gyakorlatban nagyon gyakran $e = 2^{16} + 1 = 65537$-et választanak; ez egy prím, tehát $\gcd(n, e) > 1$ nem valószínű, és $x^e = x^{2^{16}} \cdot x$ csak 2 tagból áll.)