Százezer dolláros prímszámok

2017. január 27.

Freud Róbert

2009. október 22: Átadták az Electronic Frontier Foundation 100000 dolláros díját egy

2009. október 22: Átadták az Electronic Frontier Foundation 100000 dolláros díját egy

prímszámért!

2009. október 22: Átadták az Electronic Frontier Foundation 100000 dolláros díját egy

prímszámért!

A díj az első olyan prímszám megtalálásáért járt, amely legalább tízmillió számjegyből áll.

2009. október 22: Átadták az Electronic Frontier Foundation 100000 dolláros díját egy

prímszámért!

A díj az első olyan prímszám megtalálásáért járt, amely legalább tízmillió számjegyből áll.

$$2^{43112609} - 1$$

2009. október 22: Átadták az Electronic Frontier Foundation 100000 dolláros díját egy

prímszámért!

A díj az első olyan prímszám megtalálásáért járt, amely legalább tízmillió számjegyből áll.

$$2^{43112609} - 1$$

Ez 12978189 számjegyből áll.

2009. október 22: Átadták az Electronic Frontier Foundation 100000 dolláros díját egy

prímszámért!

A díj az első olyan prímszám megtalálásáért járt, amely legalább tízmillió számjegyből áll.

$$2^{43112609} - 1$$

Ez 12978189 számjegyből áll.

A GIMPS (Great Internet Mersenne Prime Search) találta 2008. augusztus 23-án. http://www.mersenne.org

2009. október 22: Átadták az Electronic Frontier Foundation 100000 dolláros díját egy

prímszámért!

A díj az első olyan prímszám megtalálásáért járt, amely legalább tízmillió számjegyből áll.

$$2^{43112609} - 1$$

Ez 12978189 számjegyből áll.

A GIMPS (Great Internet Mersenne Prime Search) találta 2008. augusztus 23-án. http://www.mersenne.org

A legelső legalább százmillió jegyű prím megtalálásáért 150000 dollár jár, ezen a projekten bárki elkezdhet dolgozni a GIMPS programban.

2009. október 22: Átadták az Electronic Frontier Foundation 100000 dolláros díját egy

prímszámért!

A díj az első olyan prímszám megtalálásáért járt, amely legalább tízmillió számjegyből áll.

$$2^{43112609} - 1$$

Ez 12978189 számjegyből áll.

A GIMPS (Great Internet Mersenne Prime Search) találta 2008. augusztus 23-án. http://www.mersenne.org

A legelső legalább százmillió jegyű prím megtalálásáért 150000 dollár jár, ezen a projekten bárki elkezdhet dolgozni a GIMPS programban.

A jelenlegi rekord $2^{74207281} - 1$, amely 22338618 jegyből áll.

Prímszám: olyan 1-nél nagyobb egész, amely csak 1-gyel és önmagával osztható a pozitív egészek közül.

Prímszám: olyan 1-nél nagyobb egész, amely csak 1-gyel és önmagával osztható a pozitív egészek közül.

Pl. 3, 53 prímszám, de 143 nem: $143 = 11 \cdot 13$.

Prímszám: olyan 1-nél nagyobb egész, amely csak 1-gyel és önmagával osztható a pozitív egészek közül.

Pl. 3, 53 prímszám, de 143 nem: $143 = 11 \cdot 13$.

Euklidész (kb. i.e. 300): Végtelen sok prímszám van.

Prímszám: olyan 1-nél nagyobb egész, amely csak 1-gyel és önmagával osztható a pozitív egészek közül.

Pl. 3, 53 prímszám, de 143 nem: $143 = 11 \cdot 13$.

Euklidész (kb. i.e. 300): Végtelen sok prímszám van.

2, 3, 5, 7, 11

Prímszám: olyan 1-nél nagyobb egész, amely csak 1-gyel és önmagával osztható a pozitív egészek közül.

Pl. 3, 53 prímszám, de 143 nem: $143 = 11 \cdot 13$.

Euklidész (kb. i.e. 300): Végtelen sok prímszám van.

2, 3, 5, 7, 11

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

Prímszám: olyan 1-nél nagyobb egész, amely csak 1-gyel és önmagával osztható a pozitív egészek közül.

Pl. 3, 53 prímszám, de 143 nem: $143 = 11 \cdot 13$.

Euklidész (kb. i.e. 300): Végtelen sok prímszám van.

2, 3, 5, 7, 11

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

Megoldatlan: Van-e végtelen sok ikerprím, azaz amelyek különbsége 2; (3,5), (5,7), (11,13), ...

Prímszám: olyan 1-nél nagyobb egész, amely csak 1-gyel és önmagával osztható a pozitív egészek közül.

Pl. 3, 53 prímszám, de 143 nem: $143 = 11 \cdot 13$.

Euklidész (kb. i.e. 300): Végtelen sok prímszám van.

2, 3, 5, 7, 11

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

Megoldatlan: Van-e végtelen sok ikerprím, azaz amelyek különbsége 2; (3,5), (5,7), (11,13), ...

Megoldatlan: Van-e végtelen sok $2^k - 1$ alakú prím; $2^2 - 1 = 3$, $2^3 - 1 = 7, 2^5 - 1 = 31, 2^7 - 1 = 127, \ldots$.

Prímszám: olyan 1-nél nagyobb egész, amely csak 1-gyel és önmagával osztható a pozitív egészek közül.

Pl. 3, 53 prímszám, de 143 nem: $143 = 11 \cdot 13$.

Euklidész (kb. i.e. 300): Végtelen sok prímszám van.

2, 3, 5, 7, 11

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

Megoldatlan: Van-e végtelen sok ikerprím, azaz amelyek különbsége 2; (3,5), (5,7), (11,13), ...

Megoldatlan: Van-e végtelen sok $2^k - 1$ alakú prím; $2^2 - 1 = 3$, $2^3 - 1 = 7, 2^5 - 1 = 31, 2^7 - 1 = 127, \ldots$.

Erdős Pál: Ez a kérdés talán a legnehezebb, ha nem is a legsürgősebb probléma, amivel az emberiség szemben áll.

$2^{100} - 1$

$2^{100} - 1$

$a^2 - b^2 = (a + b)(a - b)$; $2^{100} - 1 = (2^{50})^2 - 1^2 = (2^{50} - 1)(2^{50} + 1)$

$2^{100} - 1$

$a^2 - b^2 = (a+b)(a-b)$; $2^{100} - 1 = (2^{50})^2 - 1^2 = (2^{50} - 1)(2^{50} + 1)$

$2^{rs} - 1 = (2^r)^s - 1^s$ osztható $2^r - 1$-gyel, ezért $2^k - 1$ legfeljebb akkor lehet prím, ha a k kitevő is prím.

$2^{100} - 1$

$a^2 - b^2 = (a+b)(a-b)$; $2^{100} - 1 = (2^{50})^2 - 1^2 = (2^{50} - 1)(2^{50} + 1)$

$2^{rs} - 1 = (2^r)^s - 1^s$ osztható $2^r - 1$-gyel, ezért $2^k - 1$ legfeljebb akkor lehet prím, ha a k kitevő is prím.

$2^{11} - 1 = 2047 = 23 \cdot 89$.

$2^{100} - 1$

$a^2 - b^2 = (a+b)(a-b)$; $2^{100} - 1 = (2^{50})^2 - 1^2 = (2^{50} - 1)(2^{50} + 1)$

$2^{rs} - 1 = (2^r)^s - 1^s$ osztható $2^r - 1$-gyel, ezért $2^k - 1$ legfeljebb akkor lehet prím, ha a k kitevő is prím.

$2^{11} - 1 = 2047 = 23 \cdot 89$.

Mersenne listája (1644): $2^k - 1$ prím, ha $k = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, és összetett minden más 257-nél kisebb k-ra.

$2^{100} - 1$

$a^2 - b^2 = (a+b)(a-b)$; $2^{100} - 1 = (2^{50})^2 - 1^2 = (2^{50} - 1)(2^{50} + 1)$

$2^{rs} - 1 = (2^r)^s - 1^s$ osztható $2^r - 1$-gyel, ezért $2^k - 1$ legfeljebb akkor lehet prím, ha a k kitevő is prím.

$2^{11} - 1 = 2047 = 23 \cdot 89$.

Mersenne listája (1644): $2^k - 1$ prím, ha $k = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, és összetett minden más 257-nél kisebb k-ra.

Mersenne (1644): Ahhoz, hogy egy 15 vagy 20-jegyű számról megállapítsuk, prím-e vagy sem, egy egész élet ideje sem elég.

$2^{100} - 1$

$a^2 - b^2 = (a+b)(a-b)$; $2^{100} - 1 = (2^{50})^2 - 1^2 = (2^{50} - 1)(2^{50} + 1)$

$2^{rs} - 1 = (2^r)^s - 1^s$ osztható $2^r - 1$-gyel, ezért $2^k - 1$ legfeljebb akkor lehet prím, ha a k kitevő is prím.

$2^{11} - 1 = 2047 = 23 \cdot 89$.

Mersenne listája (1644): $2^k - 1$ prím, ha $k = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, és összetett minden más 257-nél kisebb k-ra.

Mersenne (1644): Ahhoz, hogy egy 15 vagy 20-jegyű számról megállapítsuk, prím-e vagy sem, egy egész élet ideje sem elég.

Lucas (1876): $2^{67} - 1$ összetett!

$2^{100} - 1$

$a^2 - b^2 = (a+b)(a-b)$; $2^{100} - 1 = (2^{50})^2 - 1^2 = (2^{50} - 1)(2^{50} + 1)$

$2^{rs} - 1 = (2^r)^s - 1^s$ osztható $2^r - 1$-gyel, ezért $2^k - 1$ legfeljebb akkor lehet prím, ha a k kitevő is prím.

$2^{11} - 1 = 2047 = 23 \cdot 89$.

Mersenne listája (1644): $2^k - 1$ prím, ha $k = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, és összetett minden más 257-nél kisebb k-ra.

Mersenne (1644): Ahhoz, hogy egy 15 vagy 20-jegyű számról megállapítsuk, prím-e vagy sem, egy egész élet ideje sem elég.

Lucas (1876): $2^{67} - 1$ összetett!

Cole (1903):

$$193\,707\,721 \cdot 761\,838\,257\,287$$

Milyen gyorsan dönthető el egy 50-jegyű számról, hogy prím vagy összetett, és ha összetett, milyen gyorsan bontható fel prímszámok szorzatára?

Milyen gyorsan dönthető el egy 50-jegyű számról, hogy prím vagy összetett, és ha összetett, milyen gyorsan bontható fel prímszámok szorzatára?

A szám kisebb, mint 10^{50}, így a keresett legkisebb osztója kisebb, mint 10^{25}.

Milyen gyorsan dönthető el egy 50-jegyű számról, hogy prím vagy összetett, és ha összetett, milyen gyorsan bontható fel prímszámok szorzatára?

A szám kisebb, mint 10^{50}, így a keresett legkisebb osztója kisebb, mint 10^{25}.

Végigosztogatjuk eddig a számokkal (elég csak a páratlanokkal, sőt csak a prímszámokkal).

Milyen gyorsan dönthető el egy 50-jegyű számról, hogy prím vagy összetett, és ha összetett, milyen gyorsan bontható fel prímszámok szorzatára?

A szám kisebb, mint 10^{50}, így a keresett legkisebb osztója kisebb, mint 10^{25}.

Végigosztogatjuk eddig a számokkal (elég csak a páratlanokkal, sőt csak a prímszámokkal).

1 másodperc alatt 10^{10} próba.

Milyen gyorsan dönthető el egy 50-jegyű számról, hogy prím vagy összetett, és ha összetett, milyen gyorsan bontható fel prímszámok szorzatára?

A szám kisebb, mint 10^{50}, így a keresett legkisebb osztója kisebb, mint 10^{25}.

Végigosztogatjuk eddig a számokkal (elég csak a páratlanokkal, sőt csak a prímszámokkal).

1 másodperc alatt 10^{10} próba.

1 nap=86400 másodperc alatt kevesebb, mint 10^{15} próba.

Milyen gyorsan dönthető el egy 50-jegyű számról, hogy prím vagy összetett, és ha összetett, milyen gyorsan bontható fel prímszámok szorzatára?

A szám kisebb, mint 10^{50}, így a keresett legkisebb osztója kisebb, mint 10^{25}.

Végigosztogatjuk eddig a számokkal (elég csak a páratlanokkal, sőt csak a prímszámokkal).

1 másodperc alatt 10^{10} próba.

1 nap=86400 másodperc alatt kevesebb, mint 10^{15} próba.

1 év alatt kevesebb, mint 10^{18} próba.

Milyen gyorsan dönthető el egy 50-jegyű számról, hogy prím vagy összetett, és ha összetett, milyen gyorsan bontható fel prímszámok szorzatára?

A szám kisebb, mint 10^{50}, így a keresett legkisebb osztója kisebb, mint 10^{25}.

Végigosztogatjuk eddig a számokkal (elég csak a páratlanokkal, sőt csak a prímszámokkal).

1 másodperc alatt 10^{10} próba.

1 nap=86400 másodperc alatt kevesebb, mint 10^{15} próba.

1 év alatt kevesebb, mint 10^{18} próba.

Így rossz esetben egymillió év alatt dönthető el, hogy a szám prím-e, egy 100-jegyű számról pedig valószínűleg a Föld kihűlése előtt sem.

Gauss (1801): A prímeknek az összetett számoktól való megkülönböztetése és az összetett számok felbontása prímtényezőik szorzatára, az egész aritmetika egyik legfontosabb és leghasznosabb problémája. A tudomány méltósága megkövetelni látszik, hogy egy ilyen híres és elegáns probléma megoldásához minden segédeszközt buzgón kifejlesszünk.

Gauss (1801): A prímeknek az összetett számoktól való megkülönböztetése és az összetett számok felbontása prímtényezőik szorzatára, az egész aritmetika egyik legfontosabb és leghasznosabb problémája. A tudomány méltósága megkövetelni látszik, hogy egy ilyen híres és elegáns probléma megoldásához minden segédeszközt buzgón kifejlesszünk.

Ma már vannak gyors módszerek annak eldöntésére, hogy egy nagy szám prím vagy összetett, de nem tudunk gyors eljárást nagy összetett számok felbontásának meghatározására.

Gauss (1801): A prímeknek az összetett számoktól való megkülönböztetése és az összetett számok felbontása prímtényezőik szorzatára, az egész aritmetika egyik legfontosabb és leghasznosabb problémája. A tudomány méltósága megkövetelni látszik, hogy egy ilyen híres és elegáns probléma megoldásához minden segédeszközt buzgón kifejlesszünk.

Ma már vannak gyors módszerek annak eldöntésére, hogy egy nagy szám prím vagy összetett, de nem tudunk gyors eljárást nagy összetett számok felbontásának meghatározására.

Így bárki gyorsan találhat két nagy prímet, amit összeszorozva a kapott összetett számot rajta kívül senki más nem tudja felbontani.

Gauss (1801): A prímeknek az összetett számoktól való megkülönböztetése és az összetett számok felbontása prímtényezőik szorzatára, az egész aritmetika egyik legfontosabb és leghasznosabb problémája. A tudomány méltósága megkövetelni látszik, hogy egy ilyen híres és elegáns probléma megoldásához minden segédeszközt buzgón kifejlesszünk.

Ma már vannak gyors módszerek annak eldöntésére, hogy egy nagy szám prím vagy összetett, de nem tudunk gyors eljárást nagy összetett számok felbontásának meghatározására.

Így bárki gyorsan találhat két nagy prímet, amit összeszorozva a kapott összetett számot rajta kívül senki más nem tudja felbontani.

Lenstra: Tegyük fel, hogy a takarítónő tévedésből kidobta a p és q számokat, de a pq szorzat megmaradt. Hogyan nyerhetjük vissza a tényezőket? Csakis a matematika vereségeként érzékelhetjük, hogy ennek legreményteljesebb módja a szeméttelep átguberálása és mnemotechnikus technikák alkalmazása.

Klasszikus titkosírás: pl. minden betű helyett a rákövetkezőt küldjük el, ezt előre egyeztetjük a partnerünkkel.

Klasszikus titkosírás: pl. minden betű helyett a rákövetkezőt küldjük el, ezt előre egyeztetjük a partnerünkkel.

Általánosan: A és B előre megegyeznek egy T titkosító kulcsban, amelynek az inverze az M megfejtő kulcs. Ekkor A az u üzenet helyett annak T szerint titkosított változatát $v = T(u)$-t küldi el. Ezután B alkalmazza a kapott v-re az M-et, és megkapja az $M(v) = u$ eredeti üzenetet.

Klasszikus titkosírás: pl. minden betű helyett a rákövetkezőt küldjük el, ezt előre egyeztetjük a partnerünkkel.

Általánosan: A és B előre megegyeznek egy T titkosító kulcsban, amelynek az inverze az M megfejtő kulcs. Ekkor A az u üzenet helyett annak T szerint titkosított változatát $v = T(u)$-t küldi el. Ezután B alkalmazza a kapott v-re az M-et, és megkapja az $M(v) = u$ eredeti üzenetet.

A nagyon bonyolult kulcsok hosszú betűsorozatokra, pontosabban az azokból átalakított óriási — mondjuk 50-jegyű — számokra vonatkoznak. A titkosítást, továbbítást, megfejtést számítógép végzi.

Klasszikus titkosírás: pl. minden betű helyett a rákövetkezőt küldjük el, ezt előre egyeztetjük a partnerünkkel.

Általánosan: A és B előre megegyeznek egy T titkosító kulcsban, amelynek az inverze az M megfejtő kulcs. Ekkor A az u üzenet helyett annak T szerint titkosított változatát $v = T(u)$-t küldi el. Ezután B alkalmazza a kapott v-re az M-et, és megkapja az $M(v) = u$ eredeti üzenetet.

A nagyon bonyolult kulcsok hosszú betűsorozatokra, pontosabban az azokból átalakított óriási — mondjuk 50-jegyű — számokra vonatkoznak. A titkosítást, továbbítást, megfejtést számítógép végzi.

A üzenetét csak B érti meg, és harmadik fél nem tud hamis üzenetet küldeni A nevében B-nek.

Klasszikus titkosírás: pl. minden betű helyett a rákövetkezőt küldjük el, ezt előre egyeztetjük a partnerünkkel.

Általánosan: A és B előre megegyeznek egy T titkosító kulcsban, amelynek az inverze az M megfejtő kulcs. Ekkor A az u üzenet helyett annak T szerint titkosított változatát $v = T(u)$-t küldi el. Ezután B alkalmazza a kapott v-re az M-et, és megkapja az $M(v) = u$ eredeti üzenetet.

A nagyon bonyolult kulcsok hosszú betűsorozatokra, pontosabban az azokból átalakított óriási — mondjuk 50-jegyű — számokra vonatkoznak. A titkosítást, továbbítást, megfejtést számítógép végzi.

A üzenetét csak B érti meg, és harmadik fél nem tud hamis üzenetet küldeni A nevében B-nek.

Probléma: nehézkes és veszélyes a kulcs előzetes egyeztetése, nem dönthetők el az A és B közötti viták, több szereplő esetén (pl. üzleti élet) minden relációban külön kulcs kell.

Diffie és Hellman (1975): Legyen T nyilvános, és csak az M titkos.

Diffie és Hellman (1975): Legyen T nyilvános, és csak az M titkos.

De ha T ismert, akkor M is!

Diffie és Hellman (1975): Legyen T nyilvános, és csak az M titkos.

De ha T ismert, akkor M is!

Legalábbis elvileg. És gyakorlatilag?

Diffie és Hellman (1975): Legyen T nyilvános, és csak az M titkos.

De ha T ismert, akkor M is!

Legalábbis elvileg. És gyakorlatilag?

Ha a titkosított üzenet pl. 2017, akkor mi volt az eredeti üzenet?

Diffie és Hellman (1975): Legyen T nyilvános, és csak az M titkos.

De ha T ismert, akkor M is!

Legalábbis elvileg. És gyakorlatilag?

Ha a titkosított üzenet pl. 2017, akkor mi volt az eredeti üzenet?

Azaz mennyi $M(2017)$, más szóval mely u-ra lesz $T(u) = 2017$?

Diffie és Hellman (1975): Legyen T nyilvános, és csak az M titkos.

De ha T ismert, akkor M is!

Legalábbis elvileg. És gyakorlatilag?

Ha a titkosított üzenet pl. 2017, akkor mi volt az eredeti üzenet?

Azaz mennyi $M(2017)$, más szóval mely u-ra lesz $T(u) = 2017$?

Kipróbáljuk: $T(1) = 2017$?, $T(2) = 2017$? stb., előbb-utóbb megtaláljuk!

Diffie és Hellman (1975): Legyen T nyilvános, és csak az M titkos.

De ha T ismert, akkor M is!

Legalábbis elvileg. És gyakorlatilag?

Ha a titkosított üzenet pl. 2017, akkor mi volt az eredeti üzenet?

Azaz mennyi $M(2017)$, más szóval mely u-ra lesz $T(u) = 2017$?

Kipróbáljuk: $T(1) = 2017$?, $T(2) = 2017$? stb., előbb-utóbb megtaláljuk!

Hát inkább utóbb, mint előbb, talán pármillió év múlva.

Diffie és Hellman (1975): Legyen T nyilvános, és csak az M titkos.

De ha T ismert, akkor M is!

Legalábbis elvileg. És gyakorlatilag?

Ha a titkosított üzenet pl. 2017, akkor mi volt az eredeti üzenet?

Azaz mennyi $M(2017)$, más szóval mely u-ra lesz $T(u) = 2017$?

Kipróbáljuk: $T(1) = 2017$?, $T(2) = 2017$? stb., előbb-utóbb megtaláljuk!

Hát inkább utóbb, mint előbb, talán pármillió év múlva.

Használható-e egy angol-magyar szótár magyar-angol szótárként?

Diffie és Hellman (1975): Legyen T nyilvános, és csak az M titkos.

De ha T ismert, akkor M is!

Legalábbis elvileg. És gyakorlatilag?

Ha a titkosított üzenet pl. 2017, akkor mi volt az eredeti üzenet?

Azaz mennyi $M(2017)$, más szóval mely u-ra lesz $T(u) = 2017$?

Kipróbáljuk: $T(1) = 2017$?, $T(2) = 2017$? stb., előbb-utóbb megtaláljuk!

Hát inkább utóbb, mint előbb, talán pármillió év múlva.

Használható-e egy angol-magyar szótár magyar-angol szótárként?

Hogy is van a „víz” angolul?

Diffie és Hellman (1975): Legyen T nyilvános, és csak az M titkos.

De ha T ismert, akkor M is!

Legalábbis elvileg. És gyakorlatilag?

Ha a titkosított üzenet pl. 2017, akkor mi volt az eredeti üzenet?

Azaz mennyi $M(2017)$, más szóval mely u-ra lesz $T(u) = 2017$?

Kipróbáljuk: $T(1) = 2017$?, $T(2) = 2017$? stb., előbb-utóbb megtaláljuk!

Hát inkább utóbb, mint előbb, talán pármillió év múlva.

Használható-e egy angol-magyar szótár magyar-angol szótárként?

Hogy is van a „víz” angolul?

A T kulcs egy valódi-titkos szótár, az M pedig egy titkos-valódi szótár; nem elég az egyiket megvenni!

Az A kulcspárja T_A, M_A, a B kulcspárja T_B, M_B, itt T_A, T_B nyilvános, de M_A-t csak az A, M_B-t csak a B ismeri (pl. a két titkos prímszáma alapján, amelyeknek csak a szorzatát teszi közzé).

Az A kulcspárja T_A, M_A, a B kulcspárja T_B, M_B, itt T_A, T_B nyilvános, de M_A-t csak az A, M_B-t csak a B ismeri (pl. a két titkos prímszáma alapján, amelyeknek csak a szorzatát teszi közzé).

Ekkor A elküldheti B-nek u helyett $v = T_B(u)$-t. Ezt csak B tudja megfejteni: $u = M_B(v)$.

Az A kulcspárja T_A, M_A, a B kulcspárja T_B, M_B, itt T_A, T_B nyilvános, de M_A-t csak az A, M_B-t csak a B ismeri (pl. a két titkos prímszáma alapján, amelyeknek csak a szorzatát teszi közzé).

Ekkor A elküldheti B-nek u helyett $v = T_B(u)$-t. Ezt csak B tudja megfejteni: $u = M_B(v)$.

De C is elküldhet A nevében ugyanígy egy hamis levelet! Ez egy névtelen levél, nincs aláírva!

Az A kulcspárja T_A, M_A, a B kulcspárja T_B, M_B, itt T_A, T_B nyilvános, de M_A-t csak az A, M_B-t csak a B ismeri (pl. a két titkos prímszáma alapján, amelyeknek csak a szorzatát teszi közzé).

Ekkor A elküldheti B-nek u helyett $v = T_B(u)$-t. Ezt csak B tudja megfejteni: $u = M_B(v)$.

De C is elküldhet A nevében ugyanígy egy hamis levelet! Ez egy névtelen levél, nincs aláírva!

Ezért A először aláír: $M_A(u)$, és utána teszi borítékba: $w = T_B(M_A(u))$-t küldi el B-nek.

Az A kulcspárja T_A, M_A, a B kulcspárja T_B, M_B, itt T_A, T_B nyilvános, de M_A-t csak az A, M_B-t csak a B ismeri (pl. a két titkos prímszáma alapján, amelyeknek csak a szorzatát teszi közzé).

Ekkor A elküldheti B-nek u helyett $v = T_B(u)$-t. Ezt csak B tudja megfejteni: $u = M_B(v)$.

De C is elküldhet A nevében ugyanígy egy hamis levelet! Ez egy névtelen levél, nincs aláírva!

Ezért A először aláír: $M_A(u)$, és utána teszi borítékba: $w = T_B(M_A(u))$-t küldi el B-nek.

Ezt B (és csak B) tudja megfejteni: $u = T_A(M_B(w))$.

Az A kulcspárja T_A, M_A, a B kulcspárja T_B, M_B, itt T_A, T_B nyilvános, de M_A-t csak az A, M_B-t csak a B ismeri (pl. a két titkos prímszáma alapján, amelyeknek csak a szorzatát teszi közzé).

Ekkor A elküldheti B-nek u helyett $v = T_B(u)$-t. Ezt csak B tudja megfejteni: $u = M_B(v)$.

De C is elküldhet A nevében ugyanígy egy hamis levelet! Ez egy névtelen levél, nincs aláírva!

Ezért A először aláír: $M_A(u)$, és utána teszi borítékba: $w = T_B(M_A(u))$-t küldi el B-nek.

Ezt B (és csak B) tudja megfejteni: $u = T_A(M_B(w))$.

Nem kell előzetes kulcsegyeztetés sem, nem lehet vita A és B között, és több szereplő esetén is mindenki a saját kulcsát alkalmazza. Ilyen rendszerek működnek az üzleti életben, ilyenek garantálják a bankkártyák biztonságát stb.

És például erre használhatók az olyan nagy prímszámok, amelyek — ha úgy tetszik — valójában nem is léteznek, csak a matematikai képzelet szülöttei.