ELTE IK Diszkrét modellek alkalmazásai

9. gyakorlat

Koch-Gömöri Richárd

2021. november 18.

Titkosítás (encryption)

Alice "password" $\Longrightarrow$ Bob

Caesar-titkosítás (Caesar-rejtjelezés)
toljuk el a betűket 1-gyel
p -> q, a -> b, ..., d -> e
titkosítás (encryption) *shift* $= 1$: "password" -> "qbttxpse"
visszafejtés (decryption) *shift* $= 1$: "qbttxpse" -> "password"

eredeti sztring: plain (a példában "password"), titkosított sztring: cipher (a példában "qbttxpse")

a *shift* $= 1$ kulccsal titkosítottunk, és az eredeti sztring csak a *shift* $= 1$ kulcs ismeretében fejthető vissza

a kulcs ugyanaz volt mindkét esetben $\Longrightarrow$ szimmetrikus kulcsú titkosítás (symmetric-key encryption), a kulcsot ilyenkor titkosítási kulcsnak (encryption key) nevezzük

Szimmetrikus titkosítás (symmetric encryption)

Alice "qbttxpse" $\Longrightarrow$ Bob

Bob: "qbttxpse" ???

Alice shift=1, "qbttxpse" $\Longrightarrow$ Bob

No.

Alice ($shift = 1$) "qbttxpse" $\Longrightarrow$ Bob ($shift = 1$)

Mi van ha nem tudják előre megbeszélni mi a kulcs?

Rivest-Shamir-Adleman (RSA) nyilvános kulcsú titkosítás

one-way function

$y = f(x)$

$x \to y$ könnyű

??? $\leftarrow y$ nehéz

m: a titkosítandó üzenetet reprezentáljuk pozitív egész számként

e, n: alkalmasan választott pozitív egészek

$c = m^e \mod n$ egy one-way function

pl. $3^1 \mod 17 = 3$, $3^2 \mod 17 = 9$, $3^3 \mod 17 = 10$,
$3^4 \mod 17 = 13$, ...

ha csak c, n, e-t ismerjük, akkor m-et nehéz megkeresni

RSA titkosítás

alkalmasan választott e, n értékekkel: $c = m^e \mod n$
(c cipher, a titkosított üzenet)

a visszafejtéshez keressünk olyan d kitevőt, amivel c-ből könnyen megkapjuk m-et:

$c^d \mod n = m$, ezt könnyű kiszámolni

a d értékét úgy kell megválasztani, hogy teljesüljön az alábbi, így a visszafejtés működése helyes: $c^d = (m^e)^d = m^{e \cdot d} = m \ (n)$

a titkosításhoz e-t használtuk, a visszafejtéshez d-t

(n, e) publikus kulcs (public key), d privát kulcs (private key)

példa

eml. titkosítás: $c = m^e \mod n$, visszafejtés: $c^d \mod n = m$

Alice: publikus kulcs: $(3233, 17)$, privát kulcs: 2753

Alice nyilvánosságra hozza a publikus kulcsát: $(3233, 17)$
Bob: titkosítsuk az $m = 65$ üzenetet
Bob: titkosítás: $c = 65^{17} \mod 3233 = 2790$
Bob "2790" $\Longrightarrow$ Alice
Alice: visszafejtés: $2790^{2753} \mod 3233 = 65$