Diszkrét matematika 2

5. előadás
Számelmélet

Mérai László
merai@inf.elte.hu
https://sites.google.com/view/laszlomerai

Komputeralgebra Tanszék

2023 ősz

Caesar kód

Ha $s = 13$ kulcsot választjuk: Rot13.
Titkosítás és kititkosítás ugyanazzal a kulccsal: $-13 \equiv 13 \mod 26$.

A titkosítás nem biztonságos: betűgyakoriság vizsgálattal törhető.

Ha a különböző pozíciókban különböző kulcsokat választhatunk (véletlenszerűen)
$\Rightarrow$ bizonyítottan biztonságos

Gyakorlatban: One Time Pad – OTP

Üzenetek: bináris formában: $\texttt{m}=100100101$
Kulcs: bináris sorozat: $\texttt{s}=010110110$
Titkosítás: bitenkénti XOR ($\mathrm{mod}\ 2$ összeadás):

$$\begin{array}{rr} & \texttt{m}=100100101 \\ \text{XOR} & \texttt{s}=010110110 \\ \hline & \texttt{c}=110010011 \end{array}$$

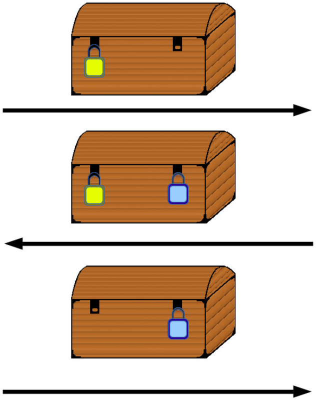
Kritikus pont: az s titkos kulcs átadása.

Nyilvános kulcsú tikosítás

- Probláma: One-time pad titkosítás során s titkos kulcs átvitele.
- Nyilvános kulcsú titkosítás: nem biztonságos csatornán közös s kulcs kiszámolása.
- Nyilvános kulcsú titkosítás kezdete: Diffie, Hellman 1976

Nyilvános kulcsú tikosítás

Nyilvános kulcsú titkosítás: nem biztonságos csatornán közös s kulcs kiszámolása.



Diffie-Hellman kulcscsere protokoll

A cél olyan $x \mapsto y$ operáció, melyet könnyű kiszámolni, de nehéz invertálni (azaz $y \mapsto x$ kiszámolása nehéz).

Diffie-Hellman: a hatványozás $k \mapsto g^k \bmod p$ könnyű, de a diszkrét logaritmus $x = g^k \mapsto \log_g x = k$ nehéz.

Diffie-Hellman kucscsere protokoll

Legyen p prímszám, és g generátor modulo p.

Alice		Bob
$a \in_R \mathbb{Z}_{p-1}$	$\xrightarrow{g^a \bmod p}$	
	$\xleftarrow{g^b \bmod p}$	$b \in_R \mathbb{Z}_{p-1}$
$\left(g^b\right)^a \bmod p =$	$g^{ab} \bmod p$	$= \left(g^a\right)^b \bmod p$

Alice és Bob $g^{ab} \bmod p$ elemet használhatja, mint közös titkos kulcsot.

$a \in_R \mathbb{Z}_{p-1}$ jelentése: a véletlenszerű választása

Diszkrét logaritmus probléma

A $x = g^k \mapsto \log_g x = k$ kiszámolása nehéz.

Példa Legyen p a következő prím ($\approx$ 1000 bites prím)

$$
\begin{aligned}
p =\ &10715086071862673209484250490600018105614048117055336074437503883703510511249\\
&36122493198378815695858127594672917553146825187145285692314043598457757469857\\
&48039345677748242309854210746050623711418779541821530464749835819412673987675\\
&59165543946077062914571196477686542167660429831652624386837205668069673;
\end{aligned}
$$

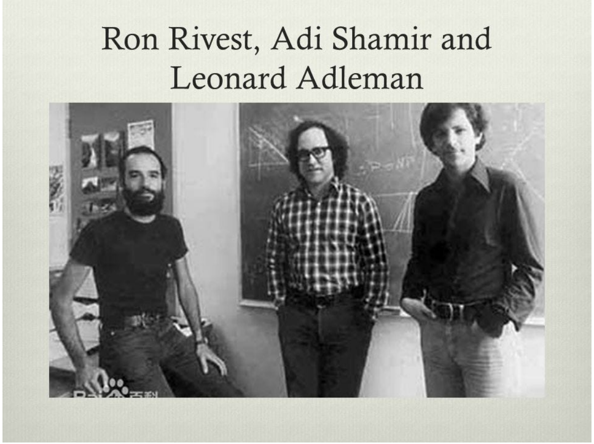
Ekkor

$$
\begin{aligned}
&\log_7 58107359726045627482630100220536377650192592471620324444843201878194251 41\\
&18190440760744898368335448696422941559188166056010735901368860071041282711306\\
&53625574092682064088312178710718876923469727146033121789183399890250919756439\\
&1668922280636877305443695008606383499842389096057545816146098541461235610 4\\
=\ &64393492197429003241377164483081335656534087098604600586356882151241561566000\\
&32109319064953874534958816025994090879400986057062706375395626849127549515157\\
&71710118982743629061168693646577971967794679154467461744044786327146512794374\\
&5260749882633574259500170050111143787375073827116865970280417108031 47
\end{aligned}
$$

RSA

A Diffie-Hellman protokoll egy kulcscsere protokoll. Hogyan tudunk titkosítani?

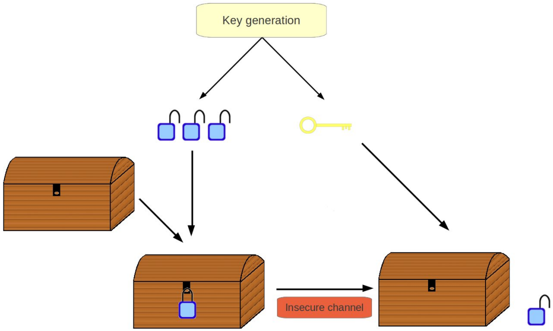
RSA: nyilvános kulcsú titkosítás, Rivest, Shamir, Aldeman 1977



Nyilvános kulcsú titkosítás

Nyilvános kulcsú titkosítás:

- Két résztvevő
- Két kulcs: titkosító kulcs (nyilvános), megfejtő kulcs (titkos)
- Titkosítani a nyilvános kulccsal, kititkosítani a tikos kulccsal



RSA

Az RSA protokol három részből áll: kulcsgenerálás, titkosítás, kititkosítás

Kulcsgenerálás

- legyen p, q két nagy prímszám és $n = p \cdot q$
- legyen $e \geq 2$, $\text{lnko}(e, \varphi(n)) = 1$
  (itt $\varphi(n) = p \cdot q \cdot (1 - 1/p) \cdot (1 - 1/q) = (p-1) \cdot (q-1)$)
- legyen d: $e \cdot d \equiv 1 \mod \varphi(n)$ (d egy lineáris kongruencia megoldása.)
- titkos kulcs: (p, q, d), nyilvános kulcs: (n, e)

Titkosítás

- legyen m egy üzenet: $1 \leq m < n$, $\text{lnko}(m, n) = 1$.
- rejtjelezett üzenet: $c = m^e \mod n$

Kititkosítás

- adott c rejtjelezett üzenet esetés $m = c^d \mod n$.

RSA helyessége

RSA:

- p, q prímek, $n = p \cdot q$,
- $e \geq 2$, $(e, \varphi(n)) = 1$
- d: $e \cdot d \equiv 1 \mod \varphi(n)$
- $c = m^e \mod n$, $m = c^d \mod n$,

Az algoritmus helyessége: legyen $(m, n) = 1$. Ekkor

$$c^d \equiv m^{ed} \equiv m^{1+k\cdot\varphi(n)} \equiv m \cdot \left(m^{\varphi(n)}\right)^k \equiv m \cdot 1^k \equiv m \mod n.$$

az Euler-Fermat tétel szerint.

Megjegyzések:

- e-t tipikus választása: $e = 2^{16} + 1$ (prímszám, gyorshatványozáshoz kényelmes)
- d kiszámolása: az $ex \equiv 1 \mod \varphi(n)$ kongruencia megoldásával

RSA példa

RSA:

- p, q prímek, $n = p \cdot q$,
- $e \geq 2$, $(e, \varphi(n)) = 1$
- d: $e \cdot d \equiv 1 \mod \varphi(n)$
- $c = m^e \bmod n$, $m = c^d \bmod n$

Példa

- Legyen $p = 11$, $q = 13$. Ekkor $n = 11 \cdot 13 = 143$ és $\varphi(143) = 11 \cdot 13 \cdot (1 - 1/11) \cdot (1 - 1/13) = (11 - 1) \cdot (13 - 1) = 120$.
- Legyen $e = 7$. Ekkor $(7, 120) = 1$.
- $7d \equiv 1 \mod 120$ megoldása: $d \equiv -17 \equiv 103 \mod 120$.
- Az $m = 3$ üzenet titkosítása: $m^e = 3^7 \equiv 42 \mod 143$
- A $c = 42$ titkos üzenet visszafejtése: $42^{103} \equiv 3 \mod 143$

RSA probléma

A titkosítás biztonságos, ha a publikus n modulusból nem lehet a titkos p, q prímeket kiszámolni (*prímfaktorizáció probléma*)

Ha p, q nagyok ($\sim 2^{1000}$), akkor ez a probléma nehéz.

Az RSALab a faktorizáció nehézségének illusztrálására 1991-ben elindította az RSA challenge kihívást:

RSA modulus	**decimális számjegyek száma**	**bitek száma**	**Díj**	**feltörve**
RSA-100	100	330	US $1,000	1991.04.01
RSA-110	110	364	US $4,429	1992.04.14
RSA-576	174	576	US $10,000	2003.12.03
RSA-640	193	640	US $20,000	2005.11.02
⋮	⋮	⋮	⋮	⋮
RSA-250	250	829	–	2020.02.28

RSA, további megjegyzések

- Hatvány kiszámolása gyors hatványozással. Például, ha $e = 2^{16} + 1$, akkor $c \equiv m^e \bmod n$ kiszámolása:

$$\Big(\big(\dots\big((m^2 \bmod n)^2 \bmod n\big)\dots\big)^2 \bmod n\Big)^2 \cdot m \bmod n$$

- Az RSA lassú. Az m üzenet tipikusan nem egy valódi üzenet (pl. szöveg), hanem egy kulcs egy gyorsabb szimmetrikus kulcsú titkosítóhoz (pl. One-time pad–OTP).
- Az RSA ebben a formában még nem biztonságos, ez csak az alapötlet.

Félévközi kérdőív

https://shorturl.at/egP49