Kriptografija i kriptoanaliza

doc. dr. sc. Ante Đerek i prof. dr. sc. Marin Golub

prosinac 2023.

Diffie-Hellmanova razmjena ključeva

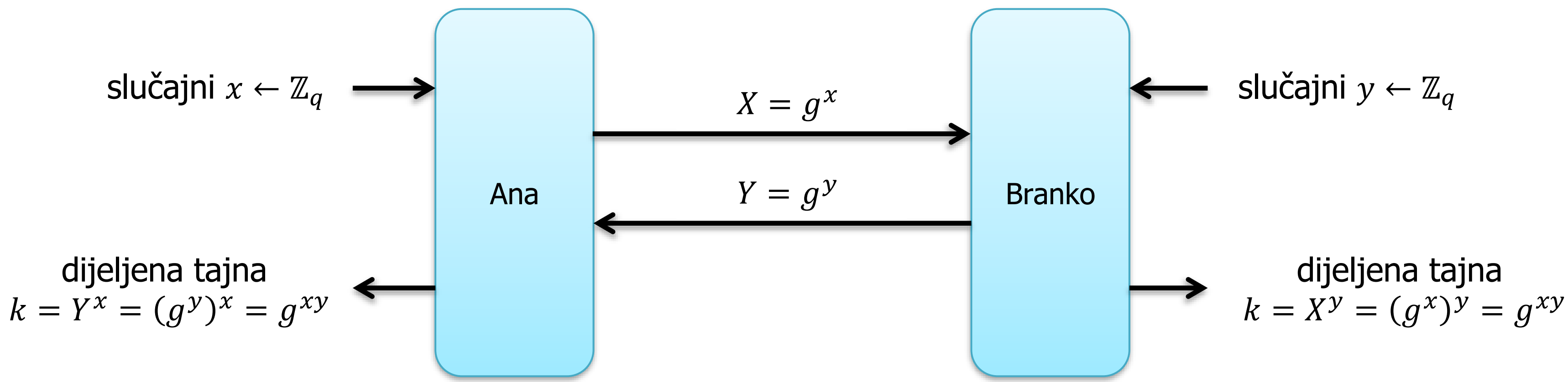
Globalni, javno poznati parametri *(domain parameters):*

- p – jako veliki prosti broj (npr. 2048 bitova)
- q – veliki prost broj koji dijeli $p-1$ (npr. 256 bitova)
- g – element od $\mathbb{Z}_p^*$ reda q

Sve operacije se rade u $\mathbb{Z}_p$ (odnosno modulo p).

Nazivlje:

- g – generator
- x – privatni ključ
- g^x – javni ključ



Diffie-Hellmanova razmjena ključeva – sigurnost

- Neformalno, Diffie-Hellmanova razmjena ključeva je *sigurna* ako je teško na temelju $X = g^x$ i $Y = g^y$ odrediti bilo što o $k = g^{xy}$.
- Pažnja: razmatramo sigurnost samo protiv *pasivnog* napadača.

Ponavljanje: Grupe

Grupe. Grupa je matematička struktura koja se sastoji od nepraznog skupa G i binarne operacije $\circ : G \times G \to G$. To znači da je za svaka dva elementa $x, y \in G$ definiran njihov umnožak $x \circ y \in G$. Pri tome zahtjevamo da vrijede sljedeća svojstva

1) **Asocijativnost.** Za sve $x, y, z \in G$ vrijedi

$$(x \circ y) \circ z = x \circ (y \circ z).$$

2) **Postojanje neutralnog elementa.** Postoji element $e \in G$ takav da za svaki $x \in G$ vrijedi

$$e \circ x = x \circ e = x.$$

3) **Postojanje inverznog elementa.** Za svaki $x \in G$ postoji element $x^{-1} \in G$ takav da je

$$x \circ x^{-1} = x^{-1} \circ x = e.$$

Ako je k tome za svaka dva elementa $x, y \in G$ ispunjeno $x \circ y = y \circ x$, onda za G kažemo da je **komutativna** ili **Abelova** grupa.

Izvor: N. Elezović, Linearna algebra 1

Primjeri grupa

- $(\mathbb{Z}, +)$ je grupa
- $(\mathbb{Q} \setminus \{0\}, *)$ je grupa
- $(\mathbb{Z}_N, +)$ je grupa
- $(\mathbb{Z}_N^*, *)$ je grupa
- ...

- $(\mathbb{N}, +)$ nije grupa
- $(\mathbb{Q}, *)$ nije grupa
- $(\mathbb{Z}_N, *)$ nije grupa ako je N složen.
- ...

Notacija

- Aditivna notacija:

$$0, a+b, -a, k\,a = a + a + \cdots + a$$

- Multiplikativna notacija:

$$1, a * b, a^{-1}, a^k = a * a * \cdots * a$$

Konačne Abelove groupe

- Grupa je *konačna* ako ima konačan broj elemenata.
- Grupa je komutativna ili Abelova ako za svaki $g, h \in G$ vrijedi $g * h = h * g$.
- U ovom predmetu kada kažemo grupa mislimo na <u>konačnu Abelovu grupu</u>.

Red elementa

- Ako je G grupa i $g \in G$.
- *Red elementa* g je veličina skupa $\{g^k : k \in \mathbb{N}\}$
  - Oznaka: $\operatorname{ord}(g)$
- Alternativno: red elementa g je najmanji prirodni broj k za koji vrijedi $g^k = 1$.

Zadatak

- Zašto alternativna definicija reda ima smisla? Je li u konačnoj grupi moguće da je $g^k \neq 1$ za sve prirodne brojeve k?

Cikličke grupe

- Neka je G grupa koja se sastoji od n elemenata. Ako postoji element $g \in G$ reda n onda kažemo da je G *ciklička grupa*.
  - $\mathrm{ord}(g) = |G|$
  - $G = \{1, g, g^2, g^3, \dots\}$
- Takav element g nazivamo *generator* ili *primitivni element* grupe G.

Primjeri cikličkih grupa

- $(\mathbb{Z}_N, +)$ je ciklička grupa
  - Npr. 1 je generator
- Ako je G bilo koja konačna grupa i $g \in G$ onda je $H = \{g, g^2, g^3, \ldots\}$ ciklička grupa. H je podgrupa od G.
- Teorem: $(\mathbb{Z}_p^*, *)$ je ciklička grupa ako je p prost.

Svojstva

- $g^{-a} := \left(g^{-1}\right)^{a}$

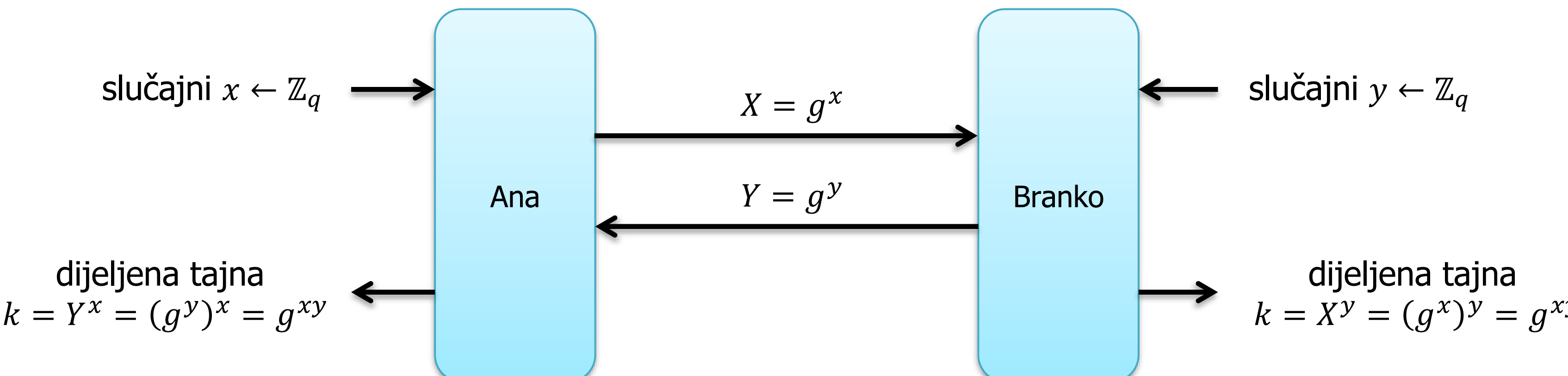
Diffie-Hellmanova razmjena ključeva u grupi G

Globalni, javno poznati parametri *(domain parameters):*

- G – konačna ciklička grupa reda q
- g – generator od G

Nazivlje:

- g – generator
- x – privatni ključ
- g^x – javni ključ



Diffie-Hellmanova razmjena ključeva – sigurnost

- Diffie-Hellmanova razmjena ključeva je sigurna ako napadač na temelju G, g, g^x, g^y ne može …
  - … odrediti g^{xy}. (*computational Diffie-Hellman assumption*)
  - … odrediti nikakve informacije o g^{xy}. (*decisional Diffie-Hellman assumption*)

Diskretni logaritam

- Diskretni logaritam u grupi G:
  - $\mathrm{Dlog}_g(h)$ je broj $k \in \mathbb{Z}$ takav da vrijedi $g^k = h$.
- Diskretni logaritam je jedinstven modulo red elementa g.

Zadatak

- Koliko je $\mathrm{Dlog}_3(11)$ u $\mathbb{Z}_{17}^*$?
- Koliko je $\mathrm{Dlog}_2(5)$ u $\mathbb{Z}_{17}^*$?

Problem diskretnog logaritma

- Neformalno, problem diskretnog logaritma je *težak* u za grupu G i generator g ako ne postoji efikasan algoritam koji računa diskretne logaritme.
- Odnos između diskretnog logaritma i Diffie-Hellmana
  - Trivijalno: Ako je diskretni logaritam lagan onda Diffie-Hellmanova razmjena ključeva nije sigurna!
  - Iskustvo: Tamo gdje je diskretni logaritam težak je i Diffie-Hellmanova razmjena ključeva sigurna!

Kada je DH siguran?

- *Prime-order subgroup*
  - G je $(\mathrm{Z}_\mathrm{p}^*, *)$ gdje je p prost
    - p je veličine npr. 2048 bitova
  - g je reda q gdje je q prost
    - q je veličine npr. 256 bitova
  - Nivo sigurnosti je oko pola veličine od q (128 bitova)
- *Safe prime* (TLS)
  - G je $(\mathrm{Z}_\mathrm{p}^*, *)$ gdje je p prost, i $(p-1)/2$ je također prost
    - p je veličine > 2048 bitova
  - g je reda $(p-1)/2$
  - Nivo sigurnosti je oko 100 bitova
- *...*

Primjer – Diffie-Hellman parametri za TLS

```
The hexadecimal representation of p is:

 FFFFFFFF FFFFFFFF ADF85458 A2BB4A9A AFDC5620 273D3CF1
 D8B9C583 CE2D3695 A9E13641 146433FB CC939DCE 249B3EF9
 7D2FE363 630C75D8 F681B202 AEC4617A D3DF1ED5 D5FD6561
 2433F51F 5F066ED0 85636555 3DED1AF3 B557135E 7F57C935
 984F0C70 E0E68B77 E2A689DA F3EFE872 1DF158A1 36ADE735
 30ACCA4F 483A797A BC0AB182 B324FB61 D108A94B B2C8E3FB
 B96ADAB7 60D7F468 1D4F42A3 DE394DF4 AE56EDE7 6372BB19
 0B07A7C8 EE0A6D70 9E02FCE1 CDF7E2EC C03404CD 28342F61
 9172FE9C E98583FF 8E4F1232 EEF28183 C3FE3B1B 4C6FAD73
 3BB5FCBC 2EC22005 C58EF183 7D1683B2 C6F34A26 C1B2EFFA
 886B4238 61285C97 FFFFFFFF FFFFFFFF

The generator is: g = 2

The group size is: q = (p-1)/2

The hexadecimal representation of q is:

 7FFFFFFF FFFFFFFF D6FC2A2C 515DA54D 57EE2B10 139E9E78
 EC5CE2C1 E7169B4A D4F09B20 8A3219FD E649CEE7 124D9F7C
 BE97F1B1 B1863AEC 7B40D901 576230BD 69EF8F6A EAFEB2B0
 9219FA8F AF833768 42B1B2AA 9EF68D79 DAAB89AF 3FABE49A
 CC278638 707345BB F15344ED 79F7F439 0EF8AC50 9B56F39A
 98566527 A41D3CBD 5E0558C1 59927DB0 E88454A5 D96471FD
 DCB56D5B B06BFA34 0EA7A151 EF1CA6FA 572B76F3 B1B95D8C
 8583D3E4 770536B8 4F017E70 E6FBF176 601A0266 941A17B0
 C8B97F4E 74C2C1FF C7278919 777940C1 E1FF1D8D A637D6B9
 9DDAFE5E 17611002 E2C778C1 BE8B41D9 6379A513 60D977FD
 4435A11C 30942E4B FFFFFFFF FFFFFFFF
```

Izvor: https://datatracker.ietf.org/doc/html/rfc7919

Diffie-Hellman parametri

Diffie–Hellman Set-up

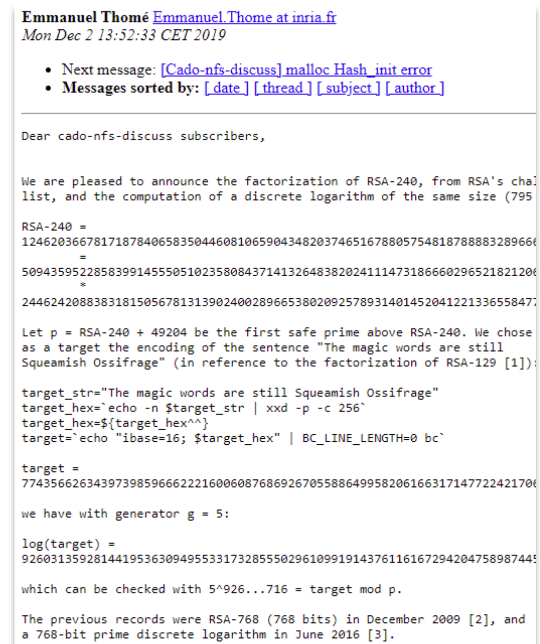
1. Choose a large prime p.
2. Choose an integer $\alpha \in \{2, 3, \ldots, p-2\}$.
3. Publish p and α.

large enough so that the index-calculus method cannot compute the DLP. By consulting Table 6.1 we see that a security level of 80 bit is achieved by primes of lengths 1024 bit, and for 128 bit security we need about 3072 bit. An additional requirement is that in order to prevent the Pohlig–Hellman attack, the order $p-1$ of the cyclic group must not factor in only small prime factors. Each of the subgroups formed by the factors of $p-1$ can be attacked using the baby-step giant-step method or Pollards's rho method, but not by the index-calculus method. Hence, the smallest prime factor of $p-1$ must be at least 160 bit long for an 80-bit security level, and at least 256 bit long for a security level of 128 bit.

Izvor: Christof Paar, Jan Pelzl, Understanding Cryptography

Diffie-Hellman – sigurnost

- Računanje diskretnog logartima je najbolji poznati općeniti napad
  - Baby-step giant-step
  - Pollardov ρ algoritam
  - Index calculus
  - General Number Field Sieve (jednako kao i za faktorizaciju)
  - U 2021. najveći izračunati Dlog je bio modulo 795-bitni prost broj.



Emmanuel Thomé Emmanuel.Thome at inria.fr
Mon Dec 2 13:52:33 CET 2019

- Next message: [Cado-nfs-discuss] malloc Hash_init error
- **Messages sorted by:** [date] [thread] [subject] [author]

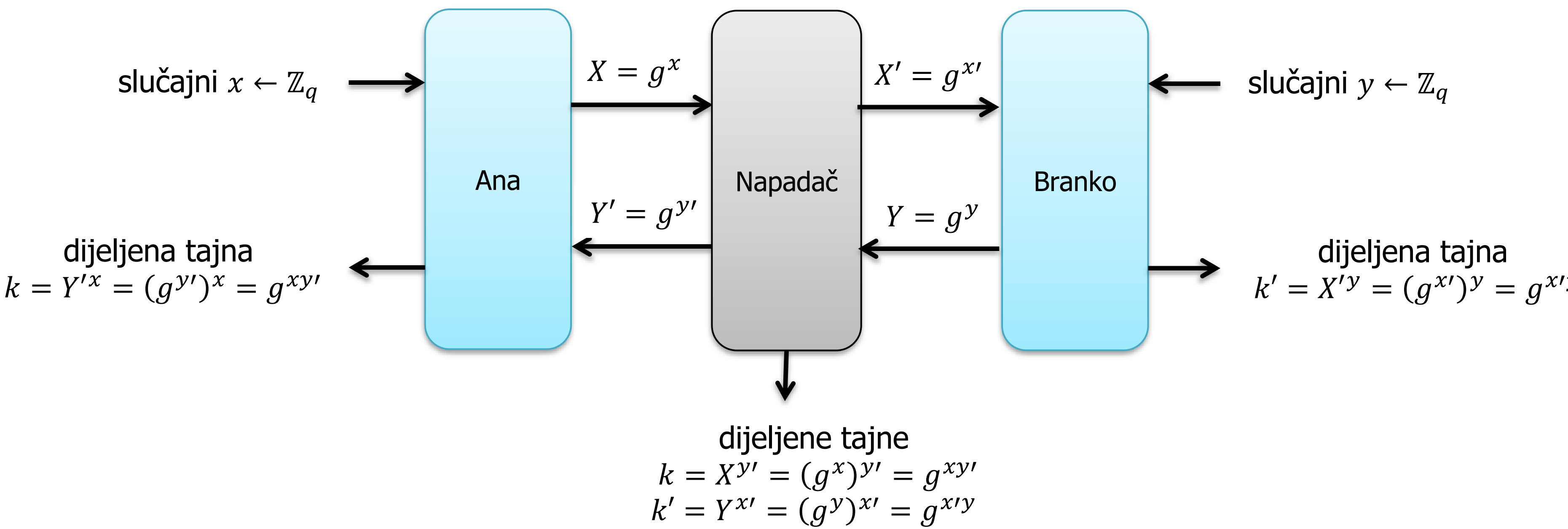
```
Dear cado-nfs-discuss subscribers,


We are pleased to announce the factorization of RSA-240, from RSA's cha
list, and the computation of a discrete logarithm of the same size (795

RSA-240 =
12462036678171878406583504460810659043482037465167880575481878888328966
        =
50943595228583991455505102358084371413264838202411147318666029652182120
        *
24462420883831815056781313902400289665380209257893140145204122133655847

Let p = RSA-240 + 49204 be the first safe prime above RSA-240. We chose
as a target the encoding of the sentence "The magic words are still
Squeamish Ossifrage" (in reference to the factorization of RSA-129 [1]):

target_str="The magic words are still Squeamish Ossifrage"
target_hex=`echo -n $target_str | xxd -p -c 256`
target_hex=${target_hex^^}
target=`echo "ibase=16; $target_hex" | BC_LINE_LENGTH=0 bc`

target =
77435662634397398596662221600608768692670558864995820616631714772242170

we have with generator g = 5:

log(target) =
92603135928144195363094955331732855502961099191437611616729420475898744

which can be checked with 5^926...716 = target mod p.

The previous records were RSA-768 (768 bits) in December 2009 [2], and
a 768-bit prime discrete logarithm in June 2016 [3].
```

Izvor: Arhiva mailing liste cado-nfs-discuss

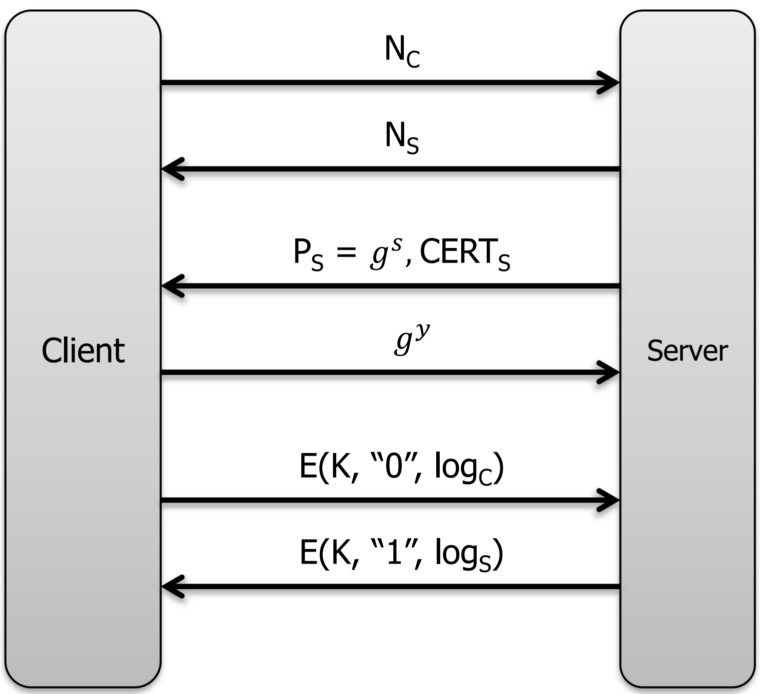
Aktivni napad

- Pažnja: Diffie-Hellmanova razmjena ključeva je sigurna samo protiv *pasivnog* napadača!
- U protokolima se koristi zajedno s digitalnim potpisima, ili nekim drugim mehanizmom za osiguravanje autentičnosti.

Napad čovjeka u sredini

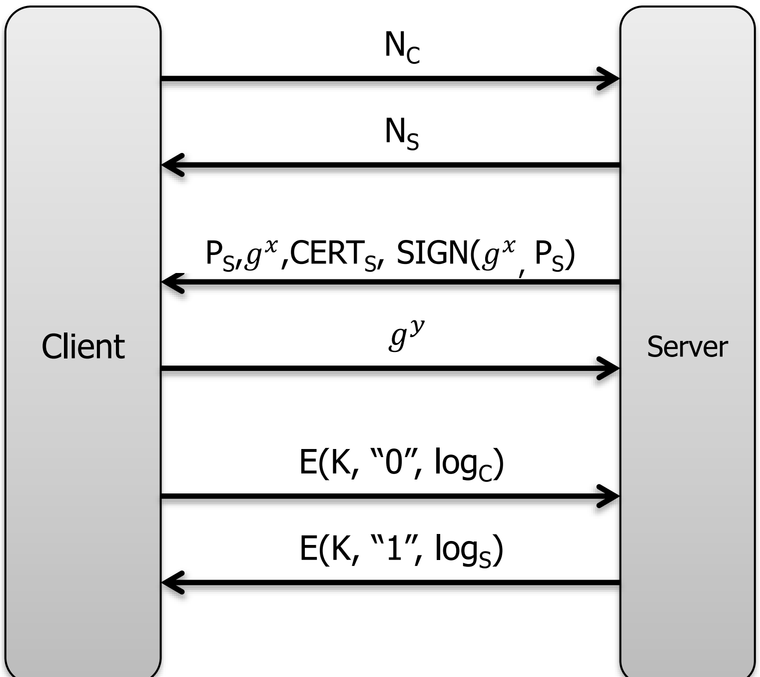


Primjena – TLS protokol – statični Diffie-Hellman



- *Fixed Diffie-Hellman*
- Javni ključ poslužitelja je zapravo Diffie-Hellman vrijednost g^s.
- Ključevi za sjednicu se generiraju na temelju Diffie-Hellman tajne i razmijenjenih *nonce* vrijednosti
- Rijetko se koristi i ne preporuča se

Primjena – TLS protokol – privremeni Diffie-Hellman



- *Ephemeral Diffie-Hellman*
- Prilikom uspostave sjednice poslužitelj i klijent razmijenjuju nove Diffie-Hellman vrijednosti.
- Ključevi za sjednicu se generiraju Diffie-Hellman tajne i razmijenjenih *nonce* vrijednosti
- Unaprijed sigurnost (*perfect forward secrecy)*
  - *Ako napadač u budućnosti kompromitira dugoročne ključeve poslužitelja, ne može dešifrirati podatke iz starih sjednica.*

Primjene

- Mnoštvo kriptografskih primitiva je bazirano na Diffie-Hellman ideji i/ili na diskretnim logaritmima
  - ElGamal asimetrična šifra
  - ElGamal digitalni potpis
  - DSA potpis
  - Schnorrovi potpisi
  - ...

ElGamalov SKJK

- Taher Elgamal (1985)
- Baziran na Diffie-Hellmanovoj razmjeni ključeva.
  - Privatni ključ je Diffie-Hellman privatni ključ
  - Javni ključ je Diffie-Hellman javni ključ
- Za svaku novu poruku, pošiljatelj generira privremene Diffie-Hellman vrijednosti i poruku kriptira tajnom dobivenom iz svojeg privremenog privatnog ključa i primateljevog dugotrajnog javnog ključa.

Obični ElGamal – generiranje ključeva

Domenski parametri:

- G ciklička grupa reda q
- g generator grupe G

Algoritam G:

1. Odaberem slučajni $a \in \mathbb{Z}_q$
2. Izračunam $\boldsymbol{A} = \boldsymbol{g}^{a}$
3. Javni ključ je $\boldsymbol{A} \in G$
4. Privatni ključ je $a \in Z_q$

Obični ElGamal – enkripcija i dekripcija

Algoritam E:

Ulaz: poruka $\boldsymbol{m} \in G$ i javni ključ $\boldsymbol{A} \in G$

1. Odaberem slučajni $y \in \mathbb{Z}_q$
2. Izračunam $\boldsymbol{Y} = \boldsymbol{g}^y$
3. Izračunam $\boldsymbol{k} = \boldsymbol{A}^y$
4. Izračunam $\boldsymbol{c} = \boldsymbol{mk}$

Rezultat je par $(\boldsymbol{Y}, \boldsymbol{c})$

Algoritam D:

Ulaz: $(\boldsymbol{Y}, \boldsymbol{c})$ i privatni ključ $a \in \mathbb{Z}_q$

1. Izračunam $\boldsymbol{k} = \boldsymbol{Y}^a$
2. Izračunam $\boldsymbol{m} = \boldsymbol{ck}^{-1}$

Rezultat je $\boldsymbol{m}$

$$D(E(m, pk), sk) = D(E(m, g^a), a) = D((g^y, mg^{ay}), a) = mg^{ay}(\mathrm{g}^{ya})^{-1} = m$$

Obični ElGamal – operacije

- Moramo znati efikasno
  - Izvršiti operaciju grupe
  - „Potenciranje” u grupi – uzastopno kvadriranje
  - Traženje inverza u grupi – svodi se na potenciranje obzirom da je poznat red grupe

Zadatak – ElGamal

- Možemo li isti privremeni par ključeva (y, g^y) koristiti dva puta?

Obični ElGamal – sigurnost

- U slučaju napada odabranim jasnim tekstom (napadač ima samo javni ključ) ElGamal je siguran ako je Diffie-Hellmanova razmjena ključeva sigurna.
- U slučaju napada odabranim skrivenim tekstom: *otvoren problem* – nemamo napade niti dokaz.

ElGamal u praksi

- Iako obični ElGamal ima puno bolja sigurnosna svojstva nego obični RSA, u praksi također gotovo nikad ne kriptiramo poruke već ga kombiniramo sa simetričnom šifrom.

Diffie-Hellman na eliptičkim krivuljama

- Pitanje za matematičare: u kojim je još grupama operacija efikasna, a problem diskretnog logaritma se čini težak?
  - Odgovor: Eliptičke krivulje zajedno s operacijom „zbrajanja” točaka.

Asimetrični kriptosustavi zasnovani na eliptičkim krivuljama (ECC)

- Sigurnost asimetričnih algoritama oslanja se na teško rješive probleme diskretnog logaritma u grupi točaka na eliptičkoj krivulji.
- Ovakve sustave su predložili 1985. godine Victor Miller i Neal Koblitz (nezavisno).
- Svaki sustav zasnovan na Diffie-Hellmanovoj razmijeni ključeva može se ostvariti nad eliptičkim krivuljama.
  - ECDH (Elliptic Curve Diffie-Hellman)
  - EC ElGamalov kriptosustav
  - ECDSA (Elliptic Curve Digital Signature Algorithm)
  - …
- Postoje eliptičkih krivulja primjene u kriptografiji koje nisu samo generalizacija algoritama na poljima – *pairing based cryptography.*

Pojednostavljena definicija eliptičke krivulje

- Eliptička krivulja E nad poljem K je skup svih točaka $(x, y) \in K \times K$ koje zadovoljavaju jednadžbu:

$$y^2 = x^3 + a\,x + b.$$

- Detalji:
  - U kriptografiji će K uglavnom biti $\mathbb{Z}_p$ gdje je p prost broj ili Galoisovo polje $GF(2^m)$.
  - U E dodamo još jedan element kojeg označavamo s 0 i nazivamo se *točka u beskonačnosti*.
  - a i b su parametri za koje vrijedi $4a^3 + 27b^2 \neq 0$ u K.

Opći oblik eliptičke krivulje
(*Weierstrassova forma*)

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$$

$a_1,a_2,a_3,a_4,a_6 \in K$ (K je algebarski zatvoreno polje)

- eliptička krivulja se može definirati nad proizvoljnim poljem K:
  - polje racionalnih brojeva Q
  - polje realnih brojeva R
  - polje kompleksnih brojeva C
  - konačno polje Z_p^*.
- *Eliptička krivulja ili nesingularna kubna krivulja* (engl. *nonsingular cubic curve*) je skup svih rješenja glatke Weierstrasseove jednadžbe
- Rješenje je točka na eliptičkoj krivulji.

Primjer – eliptička krivulja nad $\mathbb{R}$

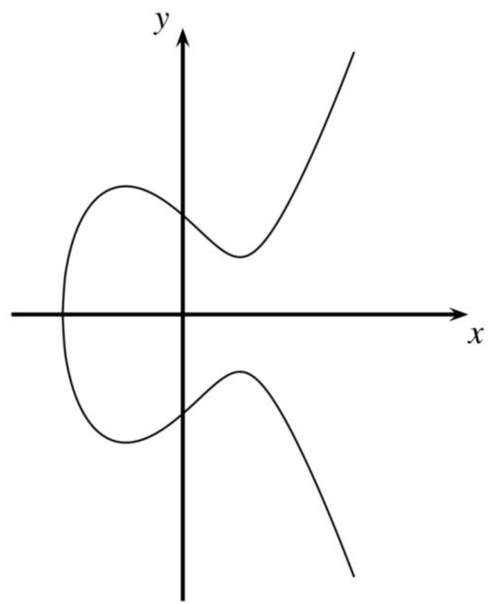
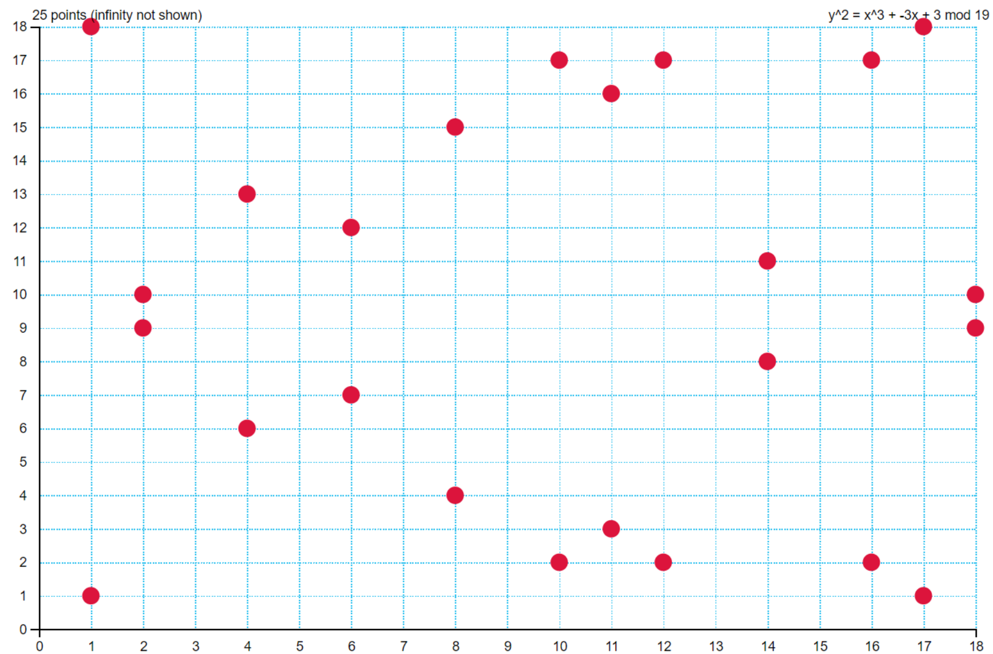


Fig. 9.3 $y^2 = x^3 - 3x + 3$ over $\mathbb{R}$

Izvor: Christof Paar, Jan Pelzl, Understanding Cryptography

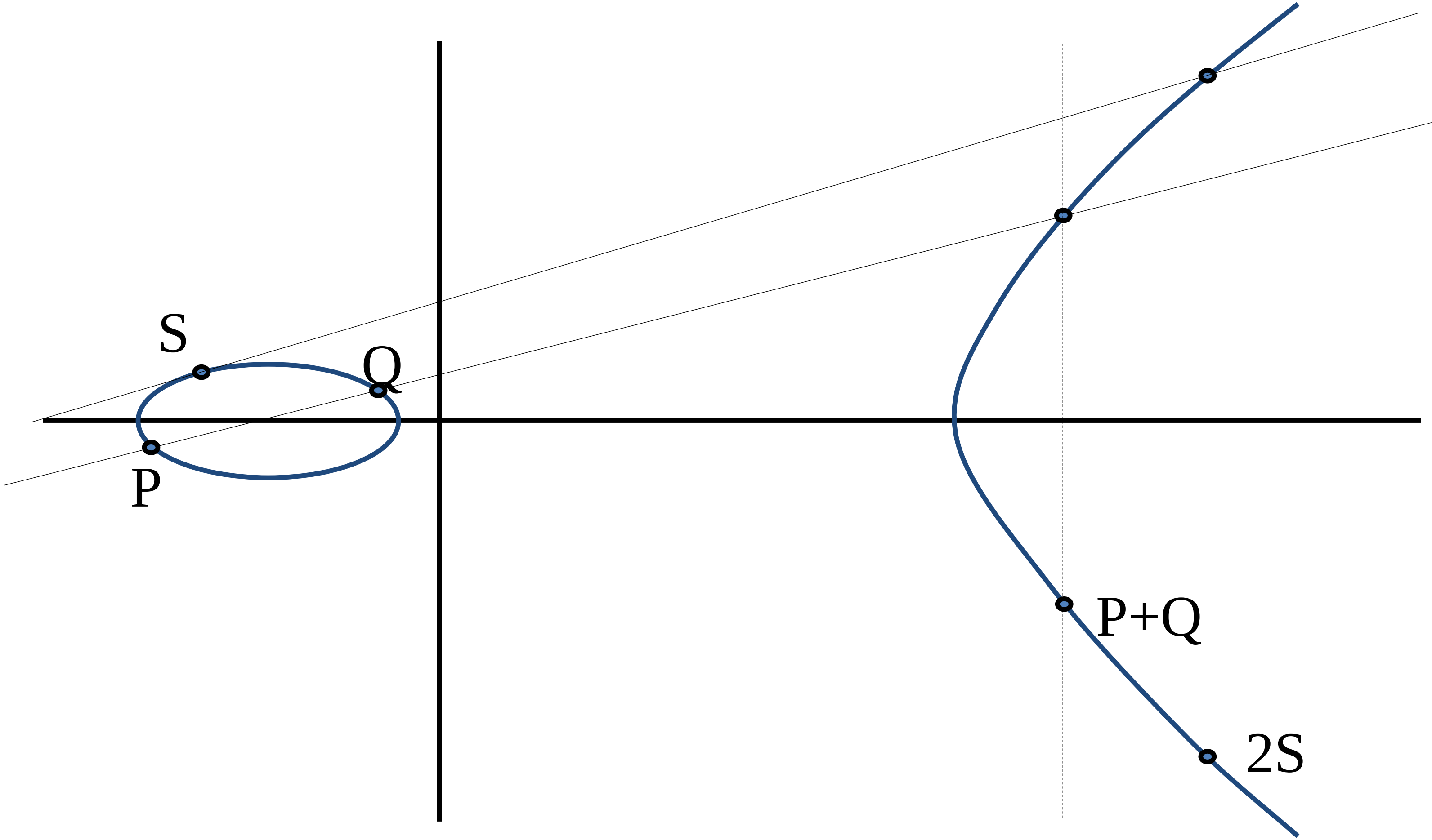
Primjer – ista krivulja nad $\mathbb{Z}_{19}$

Draw the elliptic curve $y^2 = x^3 + ax + b \mod r$, where a: -3 b: 3 r: 19 DRAW!



Izvor: https://www.graui.de/code/elliptic2/

Operacija „zbrajanja”



Operacija „zbrajanja”

$$x_3 = s^2 - x_1 - x_2 \bmod p$$
$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p \text{ ; if } P \neq Q \text{ (point addition)} \\ \frac{3x_1^2 + a}{2y_1} \bmod p \text{ ; if } P = Q \text{ (point doubling)} \end{cases}$$

- Teorem: Eliptička krivulja s ovako definiranom operacijom zbrajanja čini grupu.
- Teorem: Broj točaka na eliptičkoj krivulji nad $\mathbb{Z}_p$ je između $p + 1 - 2\sqrt{p}$ i $p + 1 + 2\sqrt{p}$.

Diskretni logaritam

- Diskretni logaritam u grupi G:
  - $\mathrm{Dlog}_g(h)$ je broj $k \in \mathbb{Z}$ takav da vrijedi $g^k = h$.
- Diskretni logaritam u grupi G točaka na eliptičkoj krivulji
  - $\mathrm{Dlog}_g(h)$ je broj $k \in \mathbb{Z}$ takav da vrijedi $kg = h$.
- Pažnja: ovo je ista stvar, samo kod eliptičkih krivulja koristimo aditivnu notaciju!

Eliptičke krivulje – sigurnost diskretnog logaritma

- Index calculus i GNFS nisu primjenjivi nad eliptičkim krivuljama.
- Za pažljivo odabrane krivulje najbolji poznati algoritmi za diskretni logaritam trebaju oko $\sqrt{n}$ koraka gdje je n veličina krivulje.
  - Baby-step giant-step
  - Pollardov ρ algoritam

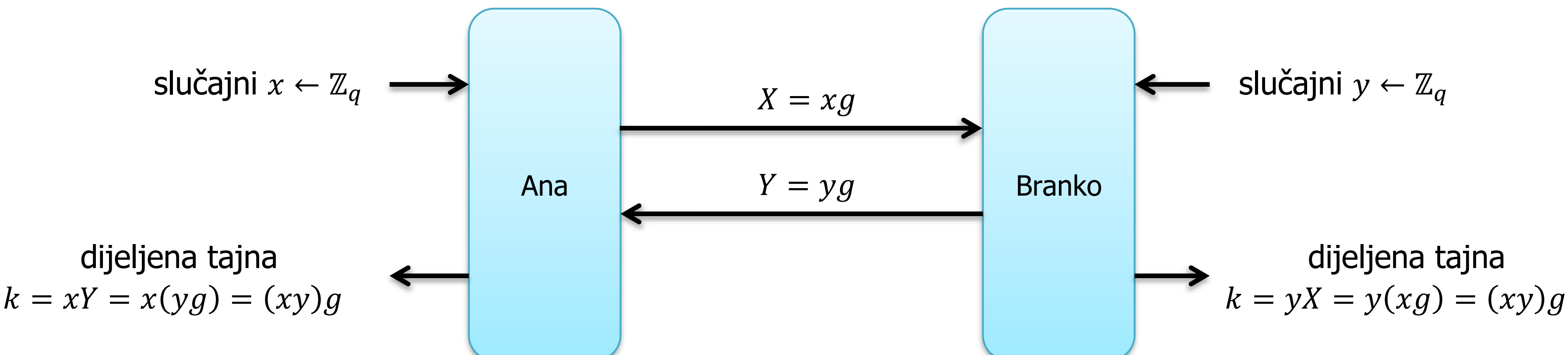
Diffie-Hellmanova razmjena nad eliptičkim krivuljama (ECDH)

Globalni, javno poznati parametri *(domain parameters):*

- G – eliptička krivulja reda q
- g – generator od G

Nazivlje:

- g – generator
- x – privatni ključ
- g^x – javni ključ



Primjer – krivulja secp256k1

The elliptic curve domain parameters over $\mathbb{F}_p$ associated with a Koblitz curve `secp256k1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

$$
\begin{aligned}
p &= \texttt{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE} \\
&\ \texttt{FFFFFC2F} \\
&= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1
\end{aligned}
$$

The curve E: $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is defined by:

$$
\begin{aligned}
a &= \texttt{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\
&\ \texttt{00000000} \\
b &= \texttt{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\
&\ \texttt{00000007}
\end{aligned}
$$

The base point G in compressed form is:

$$
\begin{aligned}
G &= \texttt{02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9} \\
&\ \texttt{59F2815B 16F81798}
\end{aligned}
$$

and in uncompressed form is:

$$
\begin{aligned}
G &= \texttt{04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9} \\
&\ \texttt{59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448} \\
&\ \texttt{A6855419 9C47D08F FB10D4B8}
\end{aligned}
$$

Finally the order n of G and the cofactor are:

$$
\begin{aligned}
n &= \texttt{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C} \\
&\ \texttt{D0364141} \\
h &= \texttt{01}
\end{aligned}
$$

Izvor: Standards for Efficient Cryptography SEC 2: Recommended Elliptic Curve Domain Parameters Certicom Research