МАТЕМАТИЧКА ГИМНАЗИЈА

МАТУРСКИ РАД

из предмета математика

Елиптичке криве и њихове примене у криптографији

Ученик:

Андрија Петровић, 4а

Ментор:

Јелена Николић

Београд, мај 2021.

0. Садржај

1.Увод

Реч криптографија води порекло од две грчке речи: криптос (*kryptós,* у преводу тајна/сакривен) и графеин (*graphein*, у преводу писати), што већ говори о старом порекли овог појма. Њена појава је разноврсна, везана за разне догађаје и периоде историје: „Енигма" машина, коришћена у Другом светском рату од стране немачке војске; Цезаров тип шифровања(Caesar cypher) где је свако слово у поруци преведено у слово фиксан број слова испред њега у алфабету; пренос вести путем робова за време античке Грчке, тако што би били записивани на њиховим главама и скривени у коси што би израсла; а неки извори приписују прву појаву старом Египту. Кроз причу наше цивилизације, видимо да је чување интегритета и приватности информација била потреба која је временом само добијала на значају.

Криптографија је наука која проучава безбедну комуникацију две стране у присуству споредне публике. Заснива се на идеји шифровања поруке(такозвани plaintext) коју желимо да пошаљемо, добијајући облик (такозвани cyphertext) неразумљив за споредну публику. Такву поруку може прочитати само циљани прималац који је способан да је дешифрује и врати у првобитни читљив облик. Енкрипција и декрипција зависе од методе, али зависе и од тајног кључа, уз који се преводи порука из једног облика у други, и без ње је то немогуће. Подразумевало се да две стране које желе да комуницирају обе већ поседују приватни кључ пре комуникације, тако да само оне могу да их шифрују и дешифрују. Тај вид криптографије се зове симетричан. Највећа мана овог облика јесте што тражи размену кључева да би се могла започети безбедна комуникација, а ако би се десило да неко пресретне приватни кључ, циљ чувања интегритета информације пада у воду.

Први видови криптографије су били лингвистичке и лексикографске основе, али временом, пративши напредак математике, области везаних за њу, појаве рачунара и интернета, шифровање је добијало јачу математичку основу, а сложеност је потекла из снаге коју је пружао компјутер. Ипак, концепт симетричне криптографије се користио све до 1970-их, док се није појавио нови облик, такозвана асиметрична криптографија (такође позната под именом „Public Key Cryptography"). Уместо једног постоје два кључа: приватни (private key) и јавни (public key). Чак и да су оба кључа интегрална за овај облик шифровања, немогуће је превести јавни у приватни. Користећи јавни кључ, свака порука се може превести у шифровани облик, али се не може превести назад у првобитни облик. То је могуће урадити само уз помоћ приватног кључа. Страна која треба да прими поруку зато шаље јавни кључ да сви могу шифровати поруке, али држи приватни кључ код себе, да једино он може да их дешифрује. Тако једна страна може да пошаље поруку коју једино друга страна може да декриптује, при се приватни кључ не излаже опасности пресретања. На овом принципу раде два веома значајна и револуционарна алгоритма: Дифе-Хелман(Diffie-Hellman) алгоритам, и РСА(RSA) алгоритам.

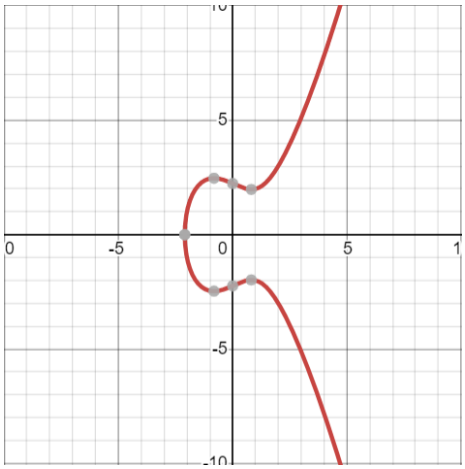
Са напретком математике, развили су се многи алгоритми асиметричне криптографије који се заснивају на разноврсним математичким принципима уз помоћ се којих и врши шифровање. Један од тих математичких принципа, и онај коме је овај рад посвећен, јесу елиптичке криве. У првим поглављима покрићемо шта су оне, неке њихове особине и теореме које из њих произилазе, понашања у зависности од поља над којима су дефинисане... Други део рада се фокусира на алгоритме, њихове особине и улогу елиптичких криви.

2.Елиптичке криве

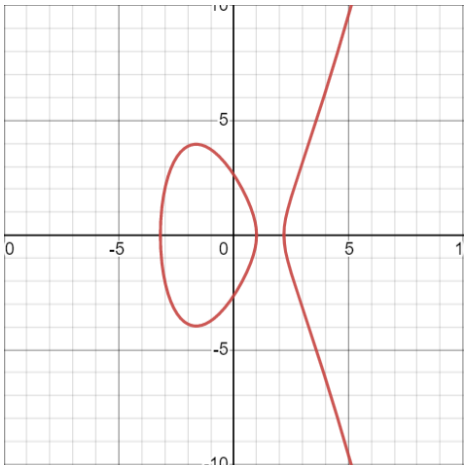
Дефиниција(Елиптичке криве): Елиптичка крива је скуп решења Вајерштрасове једначине облика:

$$Y^2 = X^3 + AX + B$$

Слика 1 и 2: Приказ две елиптичке криве у координатном систему



$1) Y^2 = X^3 - 2X + 5$



$2) Y^2 = X^3 - 8X + 7$

Битна особина елиптичких криви јесте што можемо да сабирамо тачке на њој. Ова операција се значајно разликује у односу на уобичајено сабирање, али дели неке карактеристике са њом, комутативност и асоцијативност као пример.

Прво, узмемо две тачке P и Q на елиптичкој криви E. Права која их повезује сече криву у три тачке, P, Q, и трећој коју ћемо назвати R. Тако добијену тачку R ћемо пресликати у односу на Ox осу, добијајући R' (такође ће припадати криви E, јер и (X,Y) и (X,-Y) су решења једначине). То R' ћемо назвати сумом тачака P и Q, и то записујемо у облику:

$$P \oplus Q = R'$$

(!) Мада, како будемо више користили ову операцију, израз P + Q = R' је такође валидан.

<u>Пример 1</u>: Нека је E елиптичка крива E: $Y^2 = X^3 - 7X + 10$. На њој су издвојене две тачке: P(1,2) и Q(3,4) (слика 3). Која тачка је њихов збир?

Решење: Први корак нам је да одредимо експлицитни облик праве t која повезује тачке P и Q (слика 4) :

$$k = \frac{Yp - Yq}{Xp - Xq} = \frac{2-4}{1-3} = \frac{(-2)}{(-2)} = 1 \qquad n = Yp - k * Xp = 2 - 1 * 1 = 2 - 1 = 1$$

$$\underline{t : Y = X + 1}$$

У једначину E ћемо убацити једначину праве t, тако да израчунамо њен трећи пресек са кривом, што је тачка R (слика 5) :

$(X + 1)^2 = X^3 - 7X + 10$

$X^2 + 2X + 1 = X^3 - 7X + 10$

P(X) = $X^3 - X^2 - 9X + 9 = 0$

У доминантном броју случајева, параметри криве и координате тачака могу бити велики реални бројеви који могу знатно отежати решавање једначине трећег степена коју ћемо неминовно добити као резултат. Али, јер тачке P и Q припадају правој t, и њена су решења, њихове X координате биће два од укупно три реална корена те једначине, што знатно олакшава факторизацију:

$P(1) = 1^3 - 1^2 - 9 * 1 + 9 = 1 - 1 - 9 + 9 = 0 \;\; => \;\; (X - 1)|P(X)$

$P(3) = 3^3 - 3^2 - 9 * 3 + 9 = 27 - 9 - 27 + 9 = 0 => \;\; (X - 3)|P(3)$

$P(X)/((X - 1) * (X - 3)) = (X^3 - X^2 - 9X + 9)/(X^2 - 4X + 3) = X +$ 3 (нема остатка)

$P(X) = (X - 3) * (X - 1) * (X + 3)$

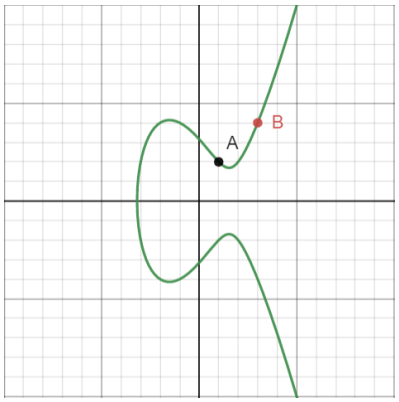
У овом облику једначине, лако видимо да је X координата треће тачке (-3), а убацивањем у једначину криве видимо да је R(-3,-2).

Последњи корак је да инвертујемо R(-3,-2) у односу на Ox осу, добијајући R'(-3,2) као крајњи резултат (слика 6)

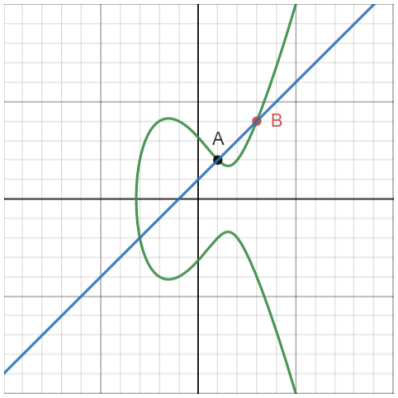
(-2)*(-1)=2

P(1,2) ⊕ Q(3,4) = R'(-3,2) ■

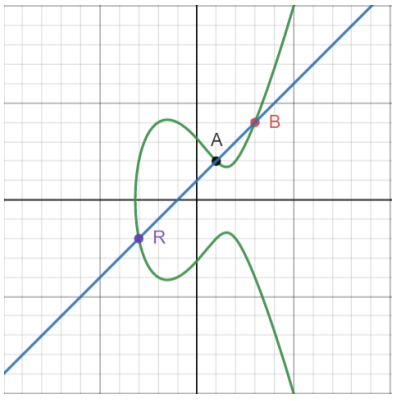
Слике 3-6 : Слике које прате кораке Примера 1



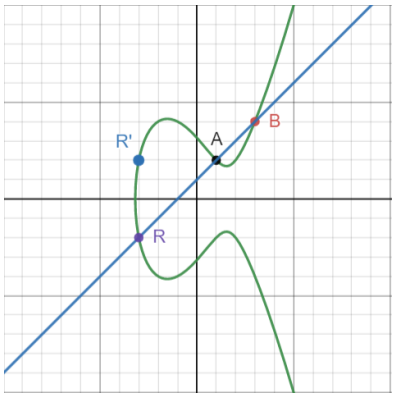
3.



4.



5.



6.

Ипак, лако је видети недостатке ове методе. Ако су две тачке исте, тојест, ако сабирамо тачку са самом собом, како би то извели? Узмимо две различите тачке, исто

као што смо узели P и Q у примеру 1. Како су те две тачке ближе једна другој на криви, видимо да права која их повезује све више тежи тангенти на график у тој тачки. Зато, када сабирамо тачку са самом собом, збир је пројекција пресека тангенте у тој тачки и криве у односу на Ox осу.

Пример 2: Дата је формула елиптичке криве E:$Y^2 = X^3 + 2X + 4$, и тачка на њој P(2,4). Која тачка је P+P?

Решење: Наћићемо коефицијент правца тангенте тако што ћемо наћи извод једначине криве:

$$(Y^2 = X^3 + 2X + 4)' = 2Y * \frac{dY}{dX} = 3X^2 + 2$$

$$\frac{dY}{dX} = k = \frac{3X^2+2}{2Y} = \frac{3*2^2+2}{2*4} = \frac{3*4+2}{8} = \frac{7}{4}$$

$$n = Y - kX = 4 - \frac{7}{4} * 2 = \frac{1}{2}$$

$$t: Y = \frac{7}{4}X + \frac{1}{2}$$

Пратећи сличан поступак као у примеру један, уврстићемо једначину тангенте у једначину криве и наћи пресек(слика 7). Током факторизације, битно је рећи да ће (X-2) бити двоструко решење, па ће ићи на квадрат.

$$\left(\frac{7}{4}X + \frac{1}{2}\right)^2 = X^3 + 2X + 4$$

$$\frac{49}{16}X^2 + \frac{7}{4}X + \frac{1}{4} = X^3 + 2X + 4$$

$$X^3 - \frac{49}{16}X^2 + \frac{1}{4}X + \frac{15}{4} = 0$$

$$16X^3 - 49X^2 + 4X + 60 = 0$$

$$(X-2)^2(16X + 15) = 0$$

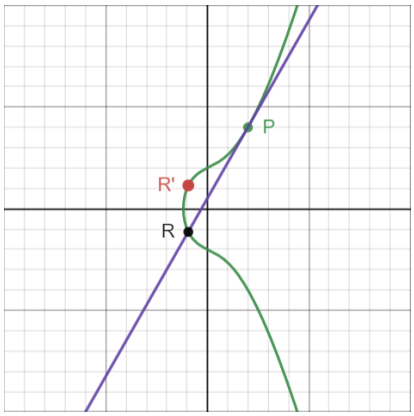
$$16(X-2)^2\left(X + \frac{15}{16}\right) = 0$$

$$\frac{7}{4} * \left(-\frac{15}{16}\right) + \frac{1}{2} = -\frac{105}{64} + \frac{32}{64} = -\frac{73}{64}$$

R$(-\frac{15}{16}-, \frac{73}{64})$

R'$(-\frac{15}{16}, \frac{73}{64})$ ■

Слика 7: Пример 2, сабирање тачке са самом собом



Такође, логично је поставити питање шта се дешава ако, кад сабирамо две тачке, права која садржи њих две не сече криву ни у једној трећој тачки? Конкретно, то је проблем код парова тачака типа (X,Y) и (X,-Y), где је права која их повезује паралелна Оу оси, па не сече нигде криву; или у проблему када је тангента у тачки паралелна са Оу осом, а сабирамо је са самом собом. Зато ћемо допунити дефиницију елиптичких криви:

Дефиниција(Елиптичка крива-допуна): Елиптичка крива је скуп решења Вајерштрасове једначине облика

$$Y^2 = X^3 + AX + B$$

укључујући и тачку О.

(При чему дискриминанта није једнака нули, тојест, важи $4A^3 + 27B^2 \neq 0$*. На крају поглавља пише зашто је ово битан услов за криптографске сврхе)*

Дефиниција(Тачка О): Тачка О припада свакој вертикалној линији у координатном систему.

Тачка О се налази „негде у бесконачности", и разумно је рећи да не припада XY координатном систему. Ипак, овако је дефинисана да решимо два превасходно поменута проблема. У првом проблему, за збир тачака P(X,Y) и Q(X,-Y), пишемо:

$$P + Q = O$$

А у другом, када је тангента тачке коју сабирамо саму са собом вертикална, назовимо је M, пишемо:

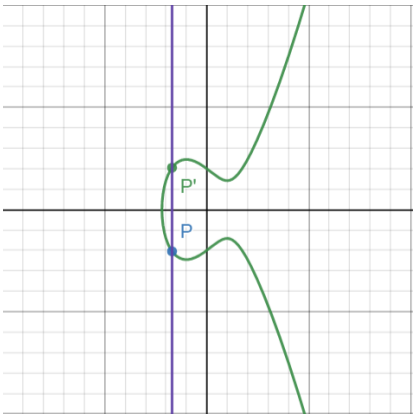
$$M + M = O$$

Како се О уклапа са осталим правилима које смо дефинисали? Да ли можемо сабирати О са нечиме? Одговор на то питање је: да.

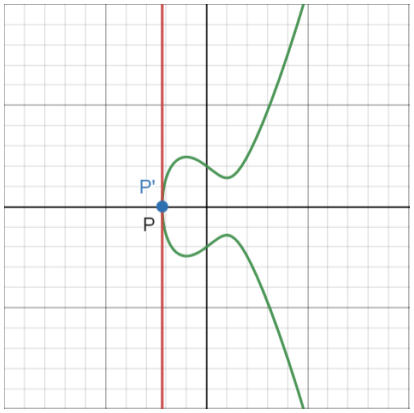
Пример 3: Дата је елиптичка крива E: $Y^2 = X^3 + AX + B$, и тачка P(X,Y) на њој. Израчунати P+O.

Решење: Како смо дефинисали, О се налази на свакој вертикалној правој. Водећи се тиме, то значи да вертикална права која пролази кроз P садржи и P, и O. То је чини њиховом повезном правом. Тада је други пресек те праве и криве тачка P'(X,-Y), инвертована слика тачке P у односу на Ox осу (слика 8). Када ту тачку инвертујемо у односу на Ox осу, као коначан збир добијамо P. Исти случај би био када би тангента у P била вертикална, јер онда би други пресек била поново тачка P (слика 9), и крајњим инвертовањем у односу на Ox осу би исто завршили у тачки P. Тако да је P+O=P. ■

Слике 8 и 9: Пример 3



8.



9.

Теорема: Операција сабирања над скупом тачака елиптичке криве E чини Абелову групу.

Доказ: Да би доказали да је нека операција над неким скупом структуре Абелове групе, морамо доказати пет својстава:

1)Затвореност:

-Када сабирамо две тачке криве, ми као резултат добијамо неку тачку на њој. У допуњеној дефиницији елиптичких криви смо додали елемент O у скуп тачака, тако да и у случајевима када као резултат добијамо O, и даље не пада затвореност. Тако да, сабирање на скупу тачака елиптичке криве јесте затворена.

2)Асоцијативност:

-Доказ за асоцијативност је подужи, и служи се знањем алгебарске теорије превише широком да може без достојног увода да се објасни. Биће наведен у материјалима линк ка раду који обрађује доказ.

3)Постојање неутрала:

-У примеру 3 смо узели општи случај, и доказали да свака тачка сабрана са O даје саму себе као резултат, тако да O јесте неутрал сабирања на скупу тачака елиптичке криве E. Ако би претпоставили да постоји још једна тачка у скупу криве која има својство неутрала, то значи да повезна права која садржи ту тачку и тачку P(X,Y) такође садржи и пројекцију од P у односу на Ox осу, тојест, садржи P'(X,-Y). Једина права која одговара тим условима јесте управо вертикална права која пролази кроз P, а једина тачка која се на њој налази поред P и P', јесте управо O. Тако да инверз јесте јединствен.

4)Постојање инверза сваког елемента скупа:

-Закључили смо да је O неутрал ове операције сабирања. Инверз неке тачке би била тачка са којом у збиру даје O као резултат. Јер се O налази само на вертикалним правама, то значи да би повезна права морали повезивати ту тачку и њену пројекцију у односу на Ox осу, и лако је видети да је то једина тачка која одговара овим условима, тако да је јединствена. Као закључак, свака тачка P(X,Y) као свој инверз има тачку P'(X,-Y).

(!) Од сада, за тачку P(X,Y) када напишемо (-P), мислимо на тачку P'(X,-Y). Такође, када напишемо P $\ominus$ Q, или чешће само P – Q, то је подударно изразу P $\oplus$ (-Q).

5)Комутативност

-За две тачке P и Q на E, небитно нам је да ли пишемо P+Q или Q+P, јер две тачке јединствено одређују само једну праву. Тиме, ова група јесте комутативна. ■

Као завршницу овог поглавља, уз помоћ свих дефиниција, правила, и допуна које смо увели, извућићемо алгоритам за рачунање збира две тачке.

Теорема(Алгоритам сабирања елиптичке криве): Нека је E елиптичка крива облика

$$E: Y^2 = X^3 + AX + B$$

а P1 и P2 неке тачке на њој. Тада:

1) Ако је P1=O, онда је P1+P2=P2
2) Ако је P2=O, онда је P1+P2=P1
3) У супротном, записујемо P1 и P2 у облику P1(X1,Y1) и P2(X2,Y2)
4) Ако је X1=X2 и Y1=(-Y2), тада је P1+P2=O
5) У супротном, дефинишемо k као:
   - $k = \frac{Y2-Y1}{X2-X1}$, ако $P1 \neq P2$
   - $k = \frac{3X1^2+A}{2Y1}$, ако $P1 = P2$

   И такође:

   $X3 = k^2 - X1 - X2$ $\qquad\qquad$ $Y3 = k(X1 - X3) - Y1$

Онда је P1+P2=(X3,Y3)

Доказ: Прва четири поступка смо већ објаснили кроз поглавље. Пети корак дефинише коефицијент правца повезне праве за две различите тачке уз помоћ једначине $\frac{(Y2-Y1)}{(X2-X1)}$, а у другом случају, када су P1 и P2 иста тачка, онда помоћу извода једначине криве поступком који је објашњен у Примеру 2. Једначине за X3 и Y3 изводимо убацујући једначину повезне праве у једначину криве, елиминишући Y, добијајући полином трећег степена облика $X^3 - k^2X^2 + (A - 2kn)X + (B - n^2) = 0$, који факторизацијом можемо написати и у облику $(X - X1)(X - X2)(X - X3) = 0$. Изједначавајући те две стране, и гледајући коефицијенте уз X^2, добијамо једначину $X3 = k^2 - X1 - X2$ која је и наведена у алгоритму. Другу једначину добијамо из израза $k = \frac{(Y3-Y1)}{(X3-X1)}$, која се лако преводи у облик наведен у алгоритму. ■

(!) Поменули смо услов $4A^3 + 27B^2 \neq 0$ када смо радили допуну дефиниције елиптичке криве. То је зато што се ограничавамо на елиптичке криве са различитим коренима (такозване non-singular). Јер је елиптичка крива једначина трећег степена, то значи да у теорији она може да се факторише у облик $Y^2 = (X - X1)(X - X2)(X - X3)$, где су X1, X2, X3 корени елиптичке криве. Дискриминанта елиптичке криве се рачуна путем једначине $-16(4A^3 + 27B^2)$, и за њу важи:

$$-16(4A^3 + 27B^2) \neq 0 \text{ ако и само ако су } X1, X2, X3 \text{ међусобно различити}$$

А, јер коефицијент -16 не игра улогу у томе да ли дискриминанта може бити једнака нули, можемо овај закључак превести у облик

$$4A^3 + 27B^2 \neq 0 \text{ ако и само ако су } X1, X2, X3 \text{ међусобно различити}$$

Разлог за овај услов је зато што сабирање онда није оптимално за криптографске сврхе, и значајно олакшава проблем решавања шифре.

3.Елиптичке криве над коначним пољима

Дефинисали смо сабирање тачака на елиптичкој криви, не можемо још да га користимо на проблемима што представља криптографија. Зато ћемо гледати елиптичке криве над коначним пољима Fp, дефинисани над скупом целобројних остатака бројева при дељењу са датим p. Тада важи:

$$E: Y^2 = X^3 + AX + B, \text{где важи } A, B \in Fp \text{ и } 4A^3 + 27B^2 \neq 0$$

као и:

$$E(Fp) = \{(x, y): x, y \in Fp \text{ и } Y^2 = X^3 + AX + B\} \cup \{O\}$$

(!) Коначна поља Fp, такозвана Галоина поља, су поља која садрже коначан број елемената, над скупом који представљаа целобројне остатке при дељењу бројем p, при чему је он прост. Над тим скупом елемената, све аритметичке операције, попут сабирања, одузимања, множења, и дељења, задовољавају услове теорије поља.

Пример 4: Дата нам је крива $E: Y^2 = X^3 + 5X + 3$ над пољем $F11$. Убацујући све могуће вредности X у једначину криве, закључићемо колико тачака задовољава услове, приметићемо да за неке вредности X одговарају две вредности Y, док за неке вредности X не одговара ни једна вредност Y:

$X = 0 : Y^2 = 0^3 + 5 * 0 + 3 = 3 \quad Y \in \{5,6\}$

$X = 1 : Y^2 = 1^3 + 5 * 1 + 3 = 9 \quad Y \in \{3,8\}$

$X = 2 : Y^2 = 2^3 + 5 * 2 + 3 = 21 \; mod \; 11 = 10 \quad Y \in \emptyset$

$X = 3 : Y^2 = 3^3 + 5 * 3 + 3 = 45 \; mod \; 11 = 1 \quad Y \in \{1,10\}$

$X = 4 : Y^2 = 4^3 + 5 * 4 + 3 = 87 \; mod \; 11 = 10 \quad Y \in \emptyset$

$X = 5 : Y^2 = 5^3 + 5 * 5 + 3 = 153 \; mod \; 11 = 10 \quad Y \in \emptyset$

$X = 6 : Y^2 = 6^3 + 5 * 6 + 3 = 249 \; mod \; 11 = 7 \quad Y \in \emptyset$

$X = 7 : Y^2 = 7^3 + 5 * 7 + 3 = 381 \; mod \; 11 = 7 \quad Y \in \emptyset$

$X = 8 : Y^2 = 8^3 + 5 * 8 + 3 = 555 \; mod \; 11 = 5 \quad Y \in \{4,7\}$

$X = 9 : Y^2 = 9^3 + 5 * 9 + 3 = 777 \; mod \; 11 = 7 \quad Y \in \emptyset$

$X = 10 : Y^2 = 10^3 + 5 * 10 + 3 = 1053 \; mod \; 11 = 8 \quad Y \in \emptyset$

Одавде видимо да су те тачке:

$$E(F11) = \{O, (0,5), (0,6)(1,3), (1,8), (3,1), (3,10), (8,4), (8,7)\}$$

Значи да се $E(F11)$ састоји од 9 тачака. ■

(!) Скуп E(Fp) је скуп свих тачака криве E над коначним пољем Fp које задовољавају једначину криве.

Али, да ли важи затвореност код сабирања тачака елиптичке криве над пољем Fp? Ако погледамо алгоритам који смо извели на крају прве главе, који је уопштење

метода којим сабирамо тачке на криви, примећујемо да једине операције које користимо су видови сабирања и множења. Јер сабирање и множење чине Абелове групе у пољу Fp, следи да ће и новодобијена тачка бити тачка поља Fp затворености. Остаје нам да докажемо да ће још припадати криви E.

Теорема: Нека је E елиптичка крива над коначним пољем Fp, а P и Q тачке скупа E(Fp). Тада:

1)Збир тачака P и Q путем алгоритма сабирања тачака на елиптичкој криви добијамо као резултат тачку која такође припада E(Fp) (операција сабирања тачака на криви је затворена над скупом E(Fp))

2)Сабирање тачака криве које припадају скупу E(Fp) путем алгоритма за сабирање тачака представља Абелову групу.

Доказ:

1) Резултат сабирања тачака на елиптичкој криви је једнак инвертованој слици пресечне тачке те криве у односу на апсцису,а јер смо дефинисали криву над скупом тачака E(Fp), значи да ће пресек те тачке бити такође нека тачка из E(Fp). За сваку X вредност одговарају две вредности броја Y: позитивна и негативна, значи да ће и слика те тачке у односу на апсцису припадати криви, тако да јесте затворена.

2) Пошто смо доказали затвореност на операцији сабирања, за Абелову групу нам је остало да докажемо асоцијативност, постојање неутрала, јединственог инверза сваког елемента, и комутативност. На сличан начин као прошли ћемо доказати асоцијативност (исти доказ који тражи веће познавање алгебарске теорије), да је O неутрал за операцију, да је инверз сваке тачке слика те тачке у односу на апсцису, и да је операција комутативна. ■

Пример 5: Узећемо елиптичку криву из претходног примера $E: Y^2 = X^3 + 5X + 3$, дефинисана над истим коначним пољем $F11$, и на њој ћемо узети тачке $P(1,8)$ и $Q(8,7)$.

Пратећи алгоритам за сабирање тачака корак по корак, добијамо:

$$k = \frac{Y2 - Y1}{X2 - X1} = \frac{7 - 8}{8 - 1} = \frac{1}{(-7)} = \frac{1}{4} = 3$$

(!) Јер је све над пољем Fp, важи $(-7) = 11 - 7 = 4$. Израз $x = \frac{1}{4}$ значи да производ $x * 4$ по модулу 11 даје остатак 1. Провером сваког броја од 0 до 10, видимо да је тај број 3.

Даље следи:

$X3 = k^2 - X1 - X2 = 9 - 1 - 8 = 0$

$Y3 = k(X1 - X3) - Y1 = 3(1 - 0) - 8 = 3 - 8 = (-5) = 6$

Резултујућа тачка R(0,6) припада скупу тачака E(F11). ■

Исто тако смо могли да саберемо било које две тачке из скупа, укључујући сабирање њих самих са собом:

X		O	(0,5)	(0,6)	(1,3)	(1,8)	(3,1)	(3,10)	(8,4)	(8,7)
		–	–	–	–	–	–	–	–	–
O	|	O	(0,5)	(0,6)	(1,3)	(1,8)	(3,1)	(3,10)	(8,4)	(8,7)
(0,5)	|	(0,5)	(3,10)	O	(3,1)	(8,4)	(0,6)	(1,8)	(8,7)	(1,3)
(0,6)	|	(0,6)	O	(3,1)	(8,7)	(3,10)	(1,3)	(0,5)	(1,8)	(8,4)
(1,3)	|	(1,3)	(3,1)	(8,7)	(1,8)	O	(8,4)	(0,6)	(0,5)	(3,10)
(1,8)	|	(1,8)	(8,4)	(3,10)	O	(1,3)	(0,5)	(8,7)	(3,1)	(0,6)
(3,1)	|	(3,1)	(0,6)	(1,3)	(8,4)	(0,5)	(8,7)	O	(3,10)	(1,8)
(3,10)	|	(3,10)	(1,8)	(0,5)	(0,6)	(8,7)	O	(8,4)	(1,3)	(3,1)
(8,4)	|	(8,4)	(8,7)	(1,8)	(0,5)	(3,1)	(3,10)	(1,3)	(0,6)	O
(8,7)	|	(8,7)	(1,3)	(8,4)	(3,10)	(0,6)	(1,8)	(3,1)	O	(0,5)

Гледајући ову таблицу, видимо да је збир сваког од два члана из E(F11) такође члан E(F11). ■

У једначини криве над коначним пољем Fp, X може имати могућих p вредности (од 0 до p-1). За сваку ту вредност, броју Y одговарају два броја (јер је Y на квадрат, па може бити и позитивно, и негативно решење). Такође укључујемо и O у E(Fp), значи додајемо још једну тачку у скуп. Водећи се том логиком, то значи да скуп E(Fp) може чинити највише 2p+1 тачака. Али, у прошлом примеру за p=11, највећи број тачака у E(F11) је 23, а у њему има 9 тачака. Веома је непрецизна ова процена.

Уопштено, можемо рећи да се случај постојања две вредности Y за једно X дешава у 50% случајева. Насупрот том случају, може се десити да у 50% случајева не одговара ни једна вредност X броју Y. Користећи ту процену, можемо рећи да ће број тачака бити приближан броју:

$$\#\mathrm{E}(Fp) \sim 50\% * 2p + 1$$

Примењујући то на претходни пример, за p=11, то је 12 тачака. Ближе него максималан број тачака, али и даље је видно одступање од 9. Зато наводимо једну теорему без доказа:

Хасеова теорема: Нека је E елиптичка крива над коначним пољем Fp. Онда важи

$$\#E(Fp) = \text{p} + 1 - \text{tp}\text{ , где за } tp \text{ важи } |tp| \leq 2\sqrt{p} \blacksquare$$

Пример 6: Користићемо нову криву, а tp ћемо изразити на овај начин (*Пример узет из књиге ,,An Introduction to Mathematical Cryptography", страна 290.):*

$$E: Y^2 = X^3 + 4X + 6 \qquad tp = p + 1 - \#E(Fp)$$

Али нећемо је гледати конкретно над пољем F11, већ уопштено, над Fp. Убацујући разне вредности p, видимо:

p	#E(Fp)	tp	$2\sqrt{p}$
3	4	0	3,46
5	8	-2	4,47
7	11	-3	5,29
11	16	-4	6,63
13	14	0	7,21
17	15	3	8,25

За веће бројеве p, процес убацивања сваког могућег броја и испробавање вредности Y је веома неефикасно. Ова теорема не одређује тачан број тачака у скупу #E(Fp), већ даје само границу. Ипак, служећи се овом теоремом, Шоф је успео да направи алгоритам који може израчуати скуп #E(Fp) за разумно време (сложеност $(\log p)^6$). Његов алгоритам је касније био надограђен од стране Елкиса и Аткина, и данас се тај алгоритам зна под именом ,,SEA algorithm". Овај рад неће улазити дубље у то како SEA ради, јер принципи иза ње би захтевале рад независан од овог; зато ју је довољно овде само поменути, као алгоритам који има велику примену. ■

4. Проблем дискретног логартима над елиптичком кривом (ECDLP)

Проблем дискретног логаритма је познат проблем у областима везане за примену математике, тако и криптографија.

У великом броју примера везаних за криптографију, особе које желе да шифрују и размене информације се зову Алиса и Боб (због почетних слова A и B), а особа која покушава да пресретне и дешифрује информацију Ева (изведено из речи ,,eavesdropper",у преводу прислушкивач), па ћемо се служити тим именима и овде.

Идеја типичног проблема дискретног логаритма јесте да Алиса жели да шифрује број x користећи прост број p (најчешће веома велики), и одговарајући број g (такозвани примитивни корен поља Fp, и није дељив са p). Степеновање број g на x-ти степен, и од добијеног производа наћи остатак при модулу p. Резултат који добије назваће h. Преведено у једначину, то је:

$$g^x \equiv h \ (mod\ p)$$

Ева зна бројеве g, h, и p, и жели да нађе вредност од x. Један метод решавања овог проблема би био да испробава редом $g^0, g^1, g^2, g^3 \ldots$ И није тешко приметити да је то екстремно неефикасан приступ проблему, поготово ако су велики бројеви у

питању. Бољи начин би био да искористи малу Фермаову теорему, па важи $g^{p-1} \equiv 1\ (mod\ p)$, што јој може олакшати да сведе максималан број покушаја на p-2. Свакако, потребан је одређени напор да се реши овакав проблем.

Овај мисаони проблем представља идеју проблема дискретног логаритма, познат под скраћеницом DPL (Discrete Logarithm Problem). У њему се јавља операција степеновања, тојест множења. Ако би степеновање разбили на множење, добили би проблем колико пута морамо помножити g са самим собом у циљу да производ при модулу p даје h.

Како можемо применити теорију елиптичких криви на ову идеју? Можемо операцију множења заменити операцијом сабирања тачака на елиптичкој криви над пољем Fp. Тада добијамо проблем: колико пута, на криви E над коначним пољем Fp, морамо сабрати тачку P саму са собом у циљу да добијемо тачку Q. Ова варијација DPL-а се зове проблем дискретног логаритма над елиптичком кривом (Elliptic Curve Discrete Logarithm Problem, ECDLP), и доноси нову димензију DPL проблему.

Дефиниција(ECDLP): Нека је E елиптичка крива над пољем Fp, и нека су P и Q тачке из скупа E(Fp). Проблем налажења природног броја n, таквог да важи Q=nP се назива проблем дискретног логаритма над елиптичком кривом(ECDLP). Тај број обележавамо изразом:

$$n = log_P(\mathrm{Q})$$

И зовемо га елиптичким дискретним логаритмом тачке Q за основу P.

Лако је видети да ова дефиниција логаритма није уобичајена, већ да је прилагођена операцији сабирања множења тачака на криви E. Да би употпунили ту замисао, морамо две ствари напоменути:

-Прво, могуће је да тачке P и Q припадају E(Fp), али да не постоји n тако да важи Q=NP (погледати пример 7). Тада кажемо да n није дефинисано. У пракси, не дешава се да су дате тачке такве да је n недефинисано, јер Алиса, користећи тајни број n и тачку P из E(Fp) ће сигурно добити тачку Q која такође припада E(Fp) такву да важи Q=nP.

-Друго, јер E(Fp) је коначан скуп, немогуће је да скуп {P,2P,3P,…} нема тачака које се понављају. За неки број m различит од n ће важити nP=mP, значи да и n и m могу бити вредности елиптичног дискретног логаритма тачке Q за основу P, и још постоји бесконачно таквих бројева као m. Посматрајући израз nP=mP, јер су m и n различити, добијамо (m-n)P=O. За најмањи природан број s такав да важи sP=O називамо га редом тачке P. Тада, ако је n0 природан број за који важи n0*P=Q, онда су сви бројеви облика n0+s*z где z припада скупу целих бројева, решења једначине Q=nP.

Гледајући израз n0+S*Z, могли би рећи да је log_P(Q) једнак најмањем природном броју овог облика. Али, идеалније нам је да кажемо да је log_P(Q) једнак остатку при модулу s, јер онда групе функција сабирања и елиптичког дискретног логаритма чине хомоморфизам, тојест:

$$logp(\mathrm{Q1+Q2}) = logp(\mathrm{Q1}) + logp(\mathrm{Q2})$$

Пример 7: Дата нам је елиптичка крива

$$E: Y^2 = X^3 + 27X + 13$$

над коначним пољем F89. Узмемо ли тачке P(24,45) и Q(17,32) из E(F89), рачунањем и временом би видели да важи Q=14P, тако да је $logp$(Q)=14. Слично, за тачке R(63,43) и S(15,12) из E(Fp), дошли би до закључка да је R=28P и S=35P, тако да је $logp$(R)=28, а $logp$(S)=35.

Али, као што смо рекли, не морају све тачке бити умножак тачке P. У скупу E(Fp) имамо 80 тачака, али за тачку P важи 40P=O. То значи да постоји само 40 тачака таквих да је умножак од P, чинећи да за пола тачака из E(Fp) не постоји n које задовољава једначину Q=nP. ■

Ева, да би сазнала број n, мора да реши ECDLP познавајући тачке P,Q, криву E, и прост број p од коначног поља Fp. Један од метода којим може да се послужи јесте да насумице одабере природне бројеве a1,a2,a3,…,ar и b1,b2,b3,…,br који се по вредности налазе између 1 и p, и да их стави у две листе облика:

Листа 1: a1*P,a2*P,a3*P,…,ar*P

Листа 2: b1*P+Q,b2*P+Q,b3*P+Q,…,br*P+Q

Еви је онда циљ да нађе два подударна броја, један који припада првој, а други који припада другој листи, рецимо да су то бројеви ax*P = by*P+Q. Помоћу та два броја, ако их одузме, добиће (ax-by)*P=Q, што значи да је број (ax-by) један од решења једначине nP=Q. Јер су јој познате тачка P, крива E, и број p, она може да нађе број s, и тако да нађе број n. По питању комплексности, ако је r (број узетих насумице одабраних бројева) већи од $\sqrt{p}$, да кажемо приближан 3$\sqrt{p}$, онда постоји добра шанса да се наиђе на подударање неке вредности у две листе.

Ипак, постоје разни методи, тиме и алгоритми који служе за решавање ECDLP-а, али им је заједничко што је просечни број корака једнак $\sqrt{p}$, што је број корака осредњег алгоритма за решавање DLP-а. То значи да најбољи алгоритми за решавање ECDLP-а су једнаке брзине као просечан алгоритам за решавање DLP-а, и за сада не постоји алгоритам који то може да уради брже од $\sqrt{p}$ корака. Уз то, рад са елиптичким кривама тражи мање меморије него са великим бројевима (јер уместо једног огромног броја се памте две координате, или чак само једна), и кључ се лакше генерише, што су све важне особине када се разматра њихово коришћење.

5. Елиптичка Дифе-Хелман размена кључева

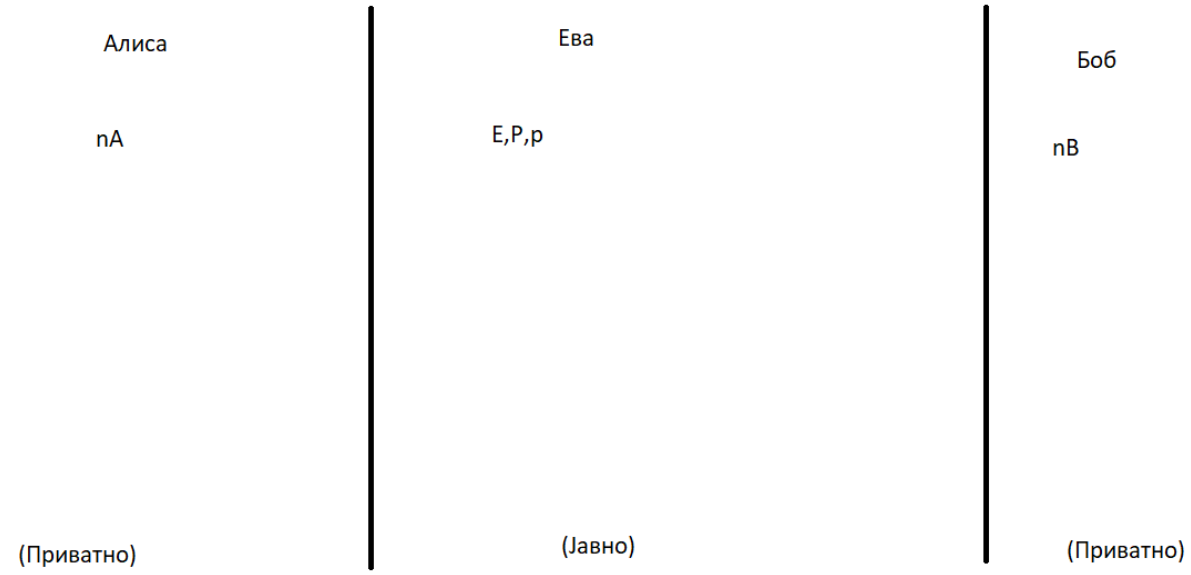
Алиса и Боб желе да безбедно размене информације, и желе да размене кључ путем ког ће моћи да само они шифрују и дешифрују поруке. Али, пут преко ког размењују информације није безбедан, јер Ева надгледа сваку поруку која се пошаље тим путем. Како Алиса и Боб могу да размене кључ тако да Ева не може да га пресретне? Један од одговора на тај проблем је Дифе-Хелманова размена кључева.

Да се надовежемо на причу у уводу, Дифе-Хелманов метод размене је један вид асиметричне криптографије. Док се није појавио овај метод, користио се само симетричан вид. Главни изазов симетричне криптографије је размена кључева између обе стране, при чему не сме бити пресретнут. То је постао знатно тежи задатак појавом интернета и мрежа, чиме је опасност пресретања постала знатно већа. Дифе-Хелманова размена је решење те препреке. Корисници неће директно слати кључ један другоме, већ путем својих приватних вредности и операција као што остатак при степеновању (DLP), или умножак неке тачке на елиптичкој криви (ECDLP), добијати резулате које

ће разменити. Ако су ти резултати пресретнути, тешко је из њих добити приватне вредности, а путем тих резултата и својих приватних вредности могу доћи до заједничког кључа познатог само њима, тако да је осигурана безбедна симетрична комуникација, а није се ниједном кључ изложио опасности.

У овом раду држаћемо се елиптичког облика ове размене, али смена операција је иста као и код DLP у ECDLP, где се множење мења сабирањем, а уместо гледања резултата при модулу p је елиптичка крива E дефинисана над коначним пољем Fp.

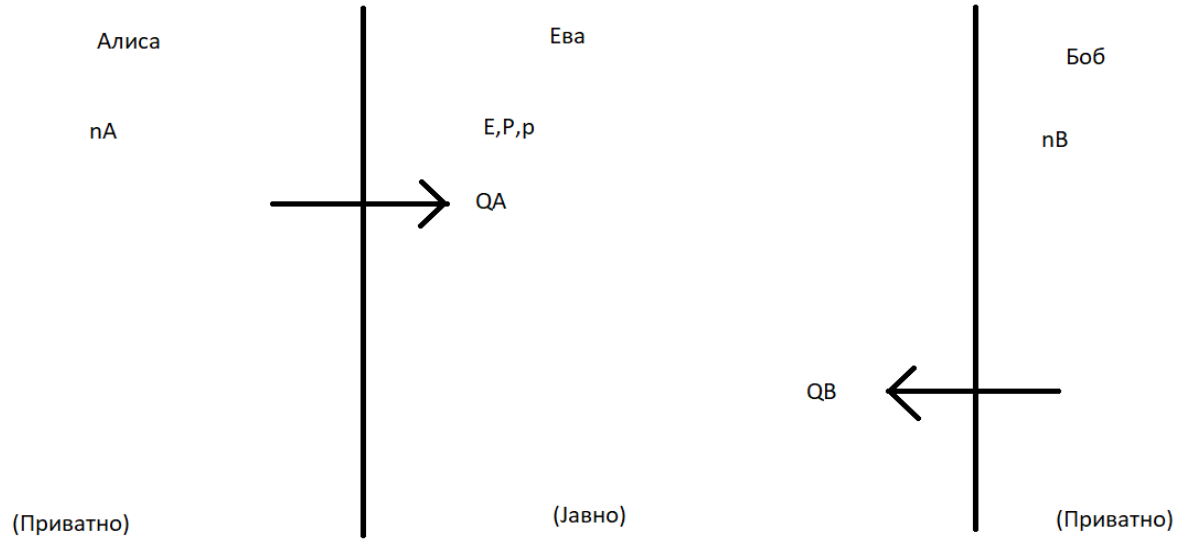
Алиса и Боб се сложе да ће користити елиптичку криву E над пољем Fp, и тачку P из скупа E(Fp) (Ова информација се гледа као јавна, тако да је и Еви ово познато. У пракси, ови параметри су објављени од једне стране, или су део неког стандарда, тако да је познато свима на тој мрежи). Алиса бира приватну вредност у облику природног броја nA, а тако исто и Боб бира nB (слика 10).



Слика 10: Елиптичка Дифе-Хелман размена кључева (Почетно стање)

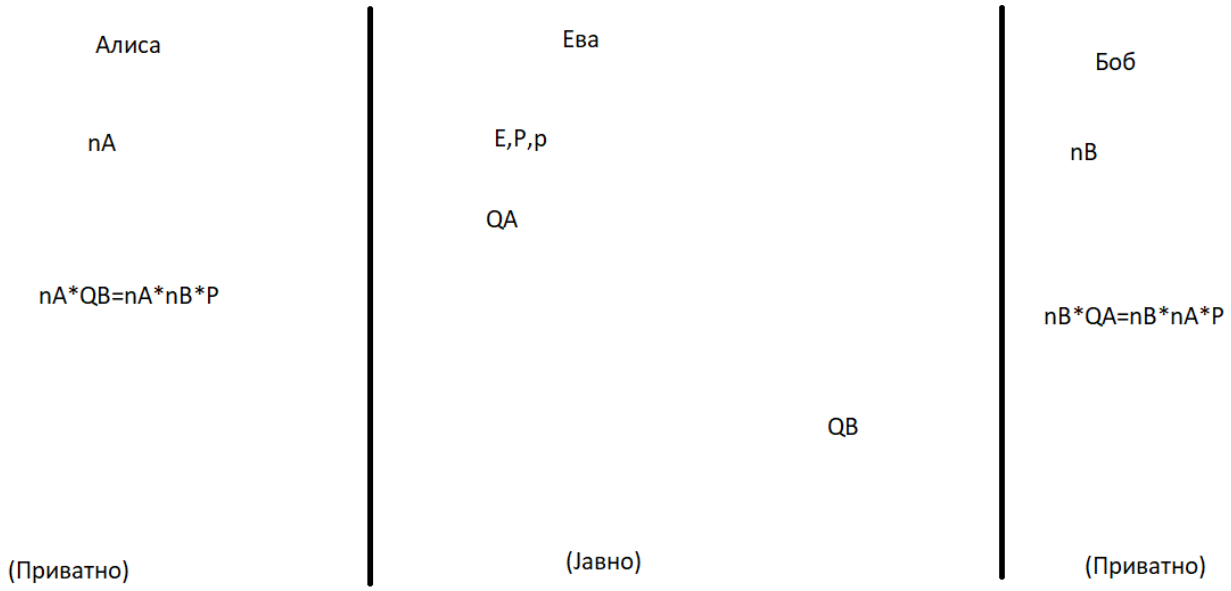
Све што је у јавном домену је познато свима, а оно што је у приватном домену је познато само онима који су у њему.

Затим, Алиса ће израчунати тачку nA*P=QA, а Боб ће тачку nB*P=QB. Те две тачке ће разменити међусобно, тако да ће и Ева моћи да их види.



Слика 11: Елиптичка Дифе-Хелман размена кључева (Размена вредности QA и QB)

На крају, Алиса када узме QB, помножиће га са својом приватном вредношћу, што је nA, а Боб ће помножити QA са nB. Тиме, Алиса ће завршити са бројем nA*QB, што је једнако nA*nB*P, а Боб ће завршити са бројем nB*QA, што је једнако nB*nA*P. Та два броја су иста, и то ће бити кључ у симетричној комуникацији између Алисе и Боба, при чему се ни једном није број nA*nB*P појавио у јавном домену да га Ева може видети.



Слика 12: Елиптичка Дифе-Хелман размена кључева (Крај)

(!) Вреди напоменути је да се не узима цела тачка као заједнички кључ, већ само вредност x координнате, не само јер нам је довољан један број, већ и због још једног разлога који ћемо показати на примеру.

Пример 8: Алиса и Боб одлуче да користе криву $E: Y^2 = X^3 + 487X + 163$ над пољем F877, и тачку P(524,729). Алиса узима број 683, док Боб узима број 758.

Алиса рачуна тачку: QA(XA,YA)=QA(79,816)

Боб рачуна тачку: QB(XB,YB)=QB(808,610)

Обоје објаве своје тачке, и прочитају другу.

Алиса добија тачку: 683*QB(808,610)=G(832,16)

Боб добија тачку: 758*QA(79,816)=G(832,16)

Обоје су завршили на истој тачки. Изостављајући Y координату из коначне тачке G, добијају број 832, који је њихов заједнички кључ. ■

Ако нам је само X координата потребна да дођемо до заједничког кључа, да ли нам је онда потребна Y координата? Рецимо да Алиса узме само X координату тачке коју добије множењем свог броја и тачке P, и само њу пошаље Бобу. Боб би могао да убаци X координату у једначину криве, и да добије две вредности Y као решење: YA и (–YA), то јест, прочитао би или QA(XA,YA), или QA'(XA, –YA), што је заправо –QA. Он не зна која је тачна вредност, тако да у пола случајева би узео QA, где би добио тачку G(XG,YG) исто као и Алиса. Ако би узео погрешну вредност QA, то јест, узео -QA, тада, при множењу те тачке са својом приватном вредношћу nB, добио би nB*(–QA)= –(nB*QA)= –(G(XG,YG))=(–G)(XG, –YG). Када гледамо G и –G, видимо да се оне разликују само по знаку испред Y координате, а да су им X координате исте, што се слаже са свиме што смо рекли у првој глави овог рада. То значи да, небитно од тога да ли је Боб узео тачан или нетачан знак за Y координату тачке QA, он ће свакако добити исту X координату, тиме и заједнички кључ, као Алиса. Овим путем, уштеђујемо још меморије, јер не морамо да шаљемо Y координату.

Пример 9: Алиса и Боб користе елиптичку криву $E: Y^2 = X^3 + 789X + 548$ над коначним пољем F941, и тачку P(367,566) из скупа E(F941). Алисина приватна вредност је nA=854, а Бобова nB=342.

Алиса добија тачку: 854*P(367,566)=QA(218,13), из које издваја X координату 218

Боб добија тачку: 342*P(367,566)=QB(396,224), из које издваја X координату 396

Алиса уноси X координату у једначину, и добија две вредности за Y: 224 и 717 (=(-224)), а Боб добија вредности 13 и 928(=(-13)). Рецимо да Алиса узима 224, што јесте тачна вредност Y координате Бобове тачке QB, али Боб је узео негативну вредност Y координате Алисине тачке QA, то јест, број 928. Множењем прочитаних тачака својим приватним вредностима

Алиса добија тачку: 854*QB(396,224)=G(740,764), и издвајањем X вредности добија 740

Боб добија тачку:342*(–QA)(218,928)=(-G)(740,177),и издвајањем X вредности добија 740

Упркос томе да Боб није имао тачне координате Алисине тачке QA, обоје су завршили са бројем 740 као заједничким кључем, тако да је размена постигла свој циљ. ■

Из перспективе Еве, њој су познате вредности QA=nA*P, QB=nB*P, крива E, тачка P, и прост број p. У случају да Алиса и Боб поделе само X координате тачака које су израчунали, то не спречава Еву да такође израчуна Y вредност, и исто тако јој неће имати великог утицаја на крајњи резултат. Она жели да пресретне кључ, и жели да нађе nA и nB, што значи да би морала да реши два ECDLP-а, један за QA, други за QB.

Други начин би био да користећи QA и QB директно из њих изведе nA*nB*P, такозвани Дифе-Хелманов проблем елиптичке криве.

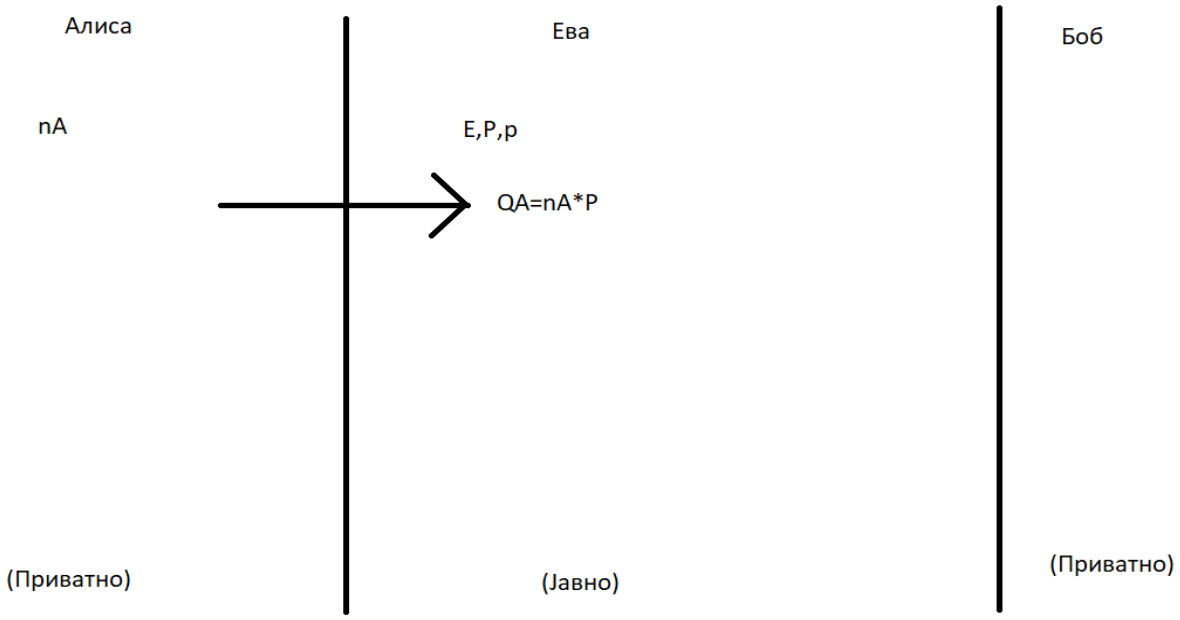
Дефиниција(Дифе-Хелманов проблем елиптичке криве): Дата нам је крива $E: Y^2 = X^3 + AX + B$ над коначним пољем Fp, и тачка P која припада скупу E(Fp). Дифе-Хелманов проблем елиптичке криве се бави извођењем вредности nA*nB*P ако су нам познате само вредности nA*P и nB*P.

У овом раду се нећемо бавити толико тим алгоритмима дешифровања, али подсетимо се да не постоји алгоритам који може да реши ECDLP проблем за мање од $\sqrt{p}$ корака. У примерима којима смо се служили смо се ограничавали на бројеве мање од хиљаду, али стандард простих бројева који се користе је да имају преко хиљаду цифара, тако да Евин изазов није ни мало наиван.

6. Елиптички ЕлГамал криптосистем

Ел Гамалов криптосистем, смишљен од стране Тахер ЕлГамала 1985. године, је један од алгоритама заснован на Дифе-Хелмановој размени кључева. Разлика између алгоритма за размену кључева и криптосистема је да првим добијамо заједничку тајну вредност, то јест тајни кључ, док другим можемо да успоставимо безбедну комуникацију. Тиме што је криптосистем, он се састоји из три компоненте: генерисање кључа, енкрипције поруке, и њене декрипције. Исто као што смо истакли код Дифе-Хелманове размене, ми ћемо објаснити њихову елиптичку варијацију, али превођењем операција сабирања тачака на криви са уобичајеним множењем, и гледање модула при дељењу бројем p, није немогуће видети како би аритметички облик изгледао. Као поставу, Алиса и Боб су се сложили да користе неки прост број p, елиптичку криву E, и тачку P из скупа E(Fp).

Генерисање кључа (Слика 13): Алиса бира приватну вредност nA, и рачуна тачку на криви Q=nA*P, која ће бити јавни кључ, и који ће проследити Бобу, тако да и Еви ће бити позната вредност Q.

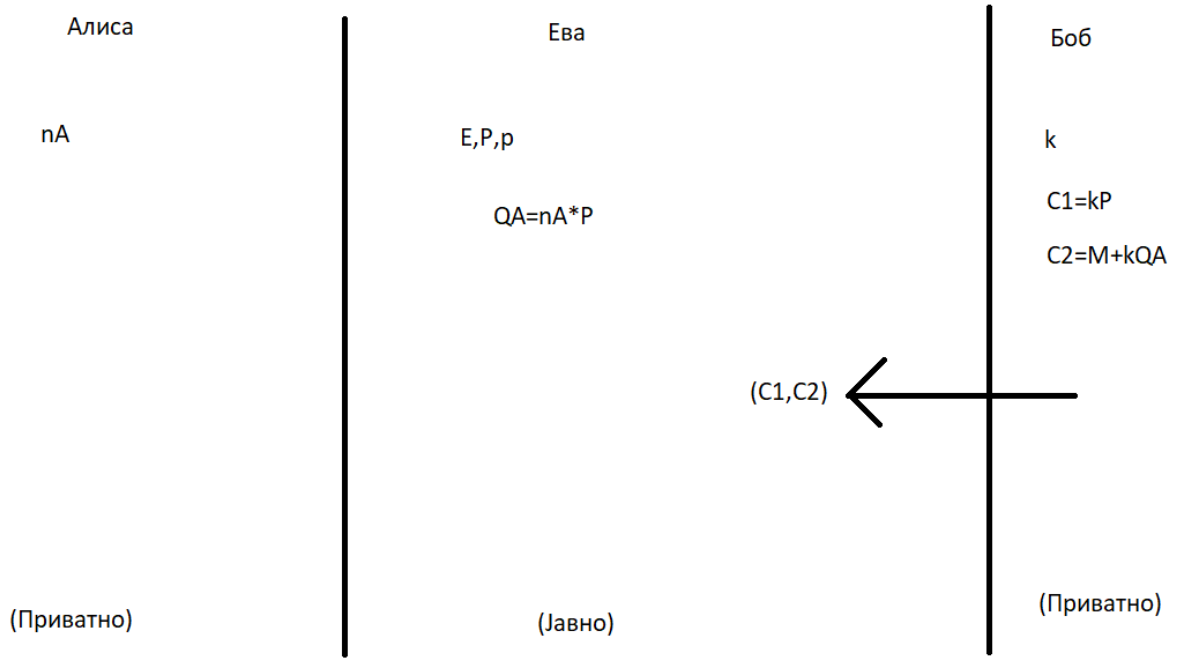


Слика 13: Ступањ генерисања јавног кључа у ЕлГамаловом криптосистему

Енкрипција (Слика 14): Боб жели да пошаље тачку M из скупа E(Fp) (То је његов plaintext, нешифрована порука. У пракси, поруке није тешко превести у форму бројева, и веома се често ради, тако да није ирационално слати бројеве као поруке, тиме ни координате неке тачке. Питање како ћемо превести поруку у тачку је проблем кога ћемо се на крају дотаћи). Он бира свој краткотрајан кључ k (такозвани ephimeral key), и путем њега, тачке P, и Алисиног јавног кључа QA, рачуна тачке:

$$C1 = kP \qquad C2 = M + kQA$$

И шаље то двоје Алиси у виду (C1,C2) као шифровану поруку (То је cyphertext)

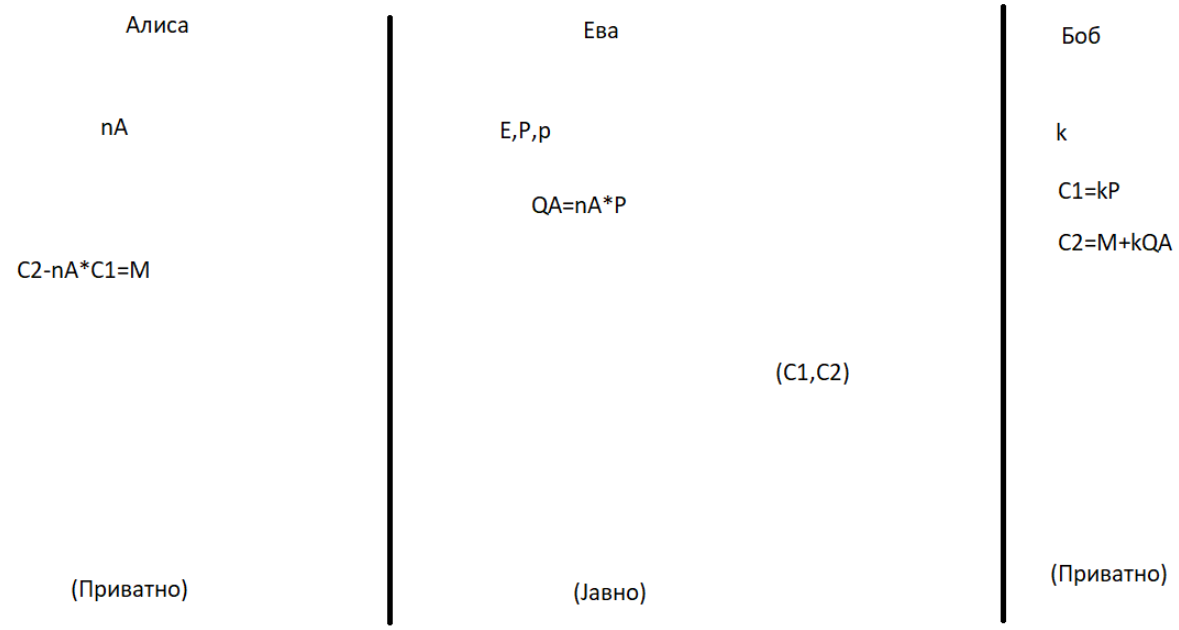


Слика 14: Ступањ енкрипције поруке у ЕлГамаловом криптосистему

Декрипција (Слика 15): Алиса, познавајући координате тачака C1 и C2, и користећи своју приватну вредност nA, ће да израчуна вредност израза $C2 - nA * C1$, којом добија:

$$C2 - nA * C1 = M + k * QA - nA * k * P = M + k * nA * P - nA * k * P = M$$

И да тиме добије вредност M, што је и био целокупни циљ овог алгоритма, при чему никада нисмо директно изложили вредност поруке M Еви, већ смо јој само остављали да решава ECDPL.



Слика 15: Ступањ декрипције поруке у ЕлГамаловом криптосистему

Постоје, ипак, две практичне непогоде када долази до ЕлГамаловог криптосистема:

1) Потешкоћа превођења поруке у шифрован облик (C1,C2)
2) Ширење поруке 4-према-1

Прва непогода је да нема ни једног на прву руку смисленог, а при том практичног начина да се преведе порука у облик две тачке (C1,C2). Једно решење тог проблема је да, уместо коришћења тачке M као шифрован облик поруке, узмемо насумичну тачку M и користимо је као маску којом ћемо шифровати поруку (начин на који то радимо је или део стандарда, или је објављен као јавна информација).

Друга непогода је што имамо 4-према-1 експанзију. Од поруке ми добијамо један број, и од тог броја касније добијамо облик (C1,C2), што значи да имамо две X координате, и две Y координате. За пренос једног броја ми носимо четири, и то није оптимално. Могли би да пробамо сличан приступ као и код Дифе-Хелман размене, а то је да шаљемо само X координате тачака, али у изразу $C2 - nA * C1$ који Алиса мора да реши, разлика између тога да ли је минус или плус у питању значајно мења резултат, тако да овај начин отпада. Ако би ову идеју хтели да применимо, треба да уз X координату пошаљемо и знак, за шта можемо резервисати још један бит, тако да практично сводимо експанзију на ниво 2-према-1. Овај метод се назива компресија тачке (point compression).

Примена ЕлГамаловог криптосистема је постојећа, али се доста користи у мешаним варијантама, тиме је и основа других принципа и алгоритама. Он фино приказује концепт постојања приватног и јавног кључа, где приватни поседује само једна страна, и путем њега само та страна може да дешифрује поруке и генерише јавни кључ путем ког друга може да шифрује своју поруку, али не може да закључи вредност приватног кључа (бар не без великог напора).

7. Крај

Како се криптографија развијала, расла је и потреба за већим бројевима и њиховим факторисањем. Били су разни методи, као што је био Полардов p-1 алгоритам за разбијање на чиниоце, и међу њима се појавио Ленстрин алгоритам током 1980-их, који се заснивао на теорији елиптичких криви, и био је превод Полардовог алгоритма на тачке елиптичке криве (исто као што смо преводили Дифе-Хелман размену и ЕлГамалов криптосистем на елиптичке варијанте мењајући операције множења бројева са сабирањем тачака на елиптичкој кривој над пољем Fp), и то је популаризовало примену елиптичких криви у криптографији. Убрзо, била је предложена идеја да оне буду основа криптосистема. Тада су се и појавиле елиптичке варијанте Дифе-Хелман и ЕлГамал алгоритма, које су биле знатно јефтиније него RCA, који је био уобичајени стандард у то време, уз чињеницу да је био први криптосистем који је настао у то време. То је привукло пажњу на њих, као и заслужен скептицизам. У то време, није се знало колико су поуздане, а ни сада се потпуно не зна да ли имају рупу у сигурности (backdoor). Током 90-их се открило да, путем MOB алгоритма, је веома лако пробити кроз суперсингуларне криве (због чега смо у првом поглављу рекли да је један од веома важних услова да дискриминанта није једнака нули), што им је потресло репутацију.

Данас се оне још проучавају, и налазе примене. Ленстрин алгоритам се и даље користи, и он је поставио основу примене Елиптичких криви. Такође (Ово нисмо поменули у првом поглављу, али је могуће да се неко досетио те могућности), јер смо рекли да могу бити дефинисане криве над свим коначним пољима облика Fp, где је p прост број, постоје поља F2 и $F2^k$ која имају своје примене и имају значајне особине. Има још таквих примера, али овај рад се ограничава на ово чему се до сада и посветио, највише због сложене математичке основе на којој се заснивају те подобласти, од којих неке би могле да заслуже рад сам за себе. Он треба да пружи основу у подскуп ове широке области, и, могуће, инспирише нечију знатижељу да лично истражи.

Материјали коришћени током писања:

Литература:

- https://www.uni-regensburg.de/Fakultaeten/nat_Fak_I/friedl/papers/elliptic_2017.pdf - „An Introduction to Mathematical Cryptography", Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

Сајтови:

- https://en.wikipedia.org/wiki/Cryptography - Википедија(Криптографија)

- https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange – Википедија (Дифе-Хелманова размена кључева)

- https://steemit.com/cryptography/@shubhamupadhyay/elliptic-curve-cryptography-or-rsa-algorithm-and-why-or-advantages-and-disadvantages (Предности и мане криптографије која се заснива на теорији елиптичких криви)

- https://crypto.stackexchange.com/questions/12864/advantages-using-diffie-hellman-or-elgamal (Дифе-Хелман у поређењу са ЕлГамалом)

- https://crypto.stackexchange.com/questions/1677/when-to-use-rsa-and-when-elgamal-asymmetric-encryption (ЕлГамал у поређењу са РСА)

Радови:

- https://www.uni-regensburg.de/Fakultaeten/nat_Fak_I/friedl/papers/elliptic_2017.pdf (Доказ да операција сабирања тачака на криви над коначним пољем Абелова група, укључује доказ асоцијативности)

Видеи:

- https://www.youtube.com/watch?v=NF1pwjL9-DE (Сабирање тачака на криви)

- https://www.youtube.com/watch?v=NmM9HA2MQGI (Дифе-Хелман, варијанта са множењем и остациме, неелиптичка варијанта)

Помагала:

- http://www.christelbach.com/ECCalculator.aspx (Калкулатор тачака на елиптичкој криви)

- https://graui.de/code/elliptic2/ (Калкулатор за број тачака у скупу E(Fp))