Сузана М. Ђорђевић
Верица Р. Милутиновић
Универзитет у Крагујевцу
Факултет педагошких наука у Јагодини
Катедра за математичко-информатичке науке

УДК 003.26:37.091.31-059.2-057.875
DOI 10.46793/Uzdanica18.II.273DJ
Оригинални научни рад
Примљен: 3. септембар 2021.
Прихваћен: 12. новембар 2021.

ПРИМЕНА КРИПТОГРАФСКОГ МОДЕЛА ЗАШТИТЕ ПОДАТАКА У ГРУПНОМ РАДУ СТУДЕНАТА[1]

Апстракт: Циљ овог рада је развијање криптографског модела за заштиту података и помагање групи студената у доношењу одлука. Групни радови су све чешћи избор наставника у провери знања студената, а због све шире употребе интернета, као и пандемије ковида 19, групни радови су се преусмерили на онлајн облик рада. Како би се спречило могуће преписивање у групама и размирице између чланова групе, потребно је развити систем који ће штитити податке, али и дозволити члановима групе да на добровољан, солидаран и демократичан начин постигну договор. Једно од могућих решења даје коришћење криптографије. За потребе развијања криптографског модела коришћена су поља Галоа GF(256) и развијане су математичке операције на пољу полинома у GF(256). Затим је у модел имплементиран Лагранжов интерполациони полином, који омогућава наставнику да генерише уређене парове који представљају део кључа. У овом раду развијен је један такав модел и приказан псеудоалгоритам за дати модел. Такође, дат је пример примене у настави програмирања.

Кључне речи: криптографија, поља Галоа, Лагранжова интерполациона формула, настава програмирања, групни рад.

УВОД

Онлајн-образовање је најопсежнији израз за описивање свих приступа учењу заснованих на технологији информационе комуникације, мада се такође користе изрази „е-учење”, „учење на даљину”, „образовање на даљину” и „учење на мрежи” (Ли 2010). Студије о онлајн-образовању показале су његов потенцијал, као и позитиван утицај на студенте захваљујући флексибилности и погодности које нуде онлајн-часови (Ален и др. 2002). Према Алену и Си-

[1] Рад је настао као резултат истраживања у оквиру билатералног пројекта „Кризе, изазови и савремени образовни систем” који реализују Факултет педагошких наука Универзитета у Крагујевцу (Србија) и Филозофски факултет Универзитета Црне Горе (Црна Гора) (2021–2023).

suzana.djordjevic@pefja.kg.ac.rs

мену (2008), више универзитета и других образовних институција пружа онлајн-образовање како би проширило своју базу студената. Према Лију (2010), популарност онлајн-образовања повећаће се у будућности јер се број онлајн курсева и програма драматично повећао током последњих година.

Како би се спречио прекид образовања током пандемије ковида 19, већина институција широм света преусмерила се на онлајн-наставу (Танхан 2020). Пандемија ковида 19 је на различите начине утицала не само на студенте, већ и ученике основних и средњих школа, родитеље, наставнике, професоре, а посебно људе са посебним потребама (Дојумгач, Танхан, Кимаз 2020). Због преласка на образовање на даљину, наставници и професори нису могли да одреде метод који би требало да усвоје, а ограничена индивидуална интеракција са ученицима закомпликовала је образовање током пандемије. Онлајн-образовање је погодно за студенте и професоре, због фактора као што су квалитет, флексибилност, осетљивост, услуге комуникације и техничке подршке (Ален и др. 2002; Танхан 2020), док истовремено доводи до одређених потешкоћа и недостатака (Танхан 2020). Танхан (2020) је утврдио да је онлајн-настава неким студентима била најбитнији водич у савладавању градива, док је другим студентима представљала највећу препреку током пандемије ковида 19. Лаки и сарадници (2019) наводе да је стопа ученика који прибегавају академским преварама у онлајн-учењу 12 пута већа од стопе у образовању лицем у лице.

Због смањеног оптерећења студената градивом, као и чињенице да омогућава неку врсту социјализације између студената у току пандемије, групни рад може бити један од најприхватљивијих модела учења. Групно учење дефинисано је као активност којом појединци стичу, деле и комбинују знање кроз своје искуство (Арготе, Груенфелд, Накуин 2001). Неке од предности групног учења су: бољи успех; продужено памћење; критичко мишљење; боља мотивација; развијање осећаја припадности; стицање социјалних вештина (Коцака, Бозана, Иуика 2009). Међутим, у условима пандемије ковида 19, реализација групног рада на до сада познат начин више није била изводљива због обавезе држања социјалне дистанце и обезбеђивања сигурности чланова групе. Решење овог проблема могло би се наћи у чињеници да је у новонасталој ситуацији знање ученика у великој мери подржано и потпомогнуто интегрисањем информационо-комуникациних технологија (ИКТ) и онлајн-ресурса (Ескобар-Родригез, Монжа-Лозано 2012). Један од њих је Мудл, софтверски пакет са материјалима отвореног кода који је бесплатан за кориснике и омогућава стварање ефикасних заједница за учење на мрежи, користећи здраве педагошке принципе. Услед чињенице да нуди бројне предности, стекао је привлачност међу наставницима и студентима (Бејти, Уласевиц 2006). Он се широко користи за подршку различитим облицима наставе као што су мешовито учење, свеприсутно учење, изокренуте учионице, групни и индивидуални рад, и водећи је софтверски пакет за учење или

управљање садржајем на северноамеричким и европским универзитетима (Костело 2013).

Један од највећих проблема код онлајн учења и оцењивања јесте преписивање, док се код онлајн групног рада могу јавити проблеми попут несугласица и неслагања чланова групе. Једно од могућих решења овог проблема може се наћи у области криптографије, чија се примена, поред обезбеђивања приватности и осигуравања података, проширила и на низ других области, па и на образовање (Виеновић, Адамовић 2013). У овом раду описује се један могући начин примене криптографског модела заштите података у организацији онлајн групног рада студената за решавање проблема у области програмирања.

ТЕОРИЈСКЕ ОСНОВЕ

У криптографији постоји много циљева, а основе за све шифарске системе јесу генератори случајних низова. За практичне системе заштите, циљ криптографа је формирање генератора псеудослучајних низова, где се при реализацији тежи ка једнозначној аутентификацији страна у комуникацији (Виеновић, Адамовић 2013). Најранији облик криптографије било је једноставно писање поруке, јер већина људи није могла да чита (Дули 2018). У ствари, сама реч *крипто̄графија* потиче од грчких речи *kryptos* (скривени) и *graphein* (писање) (Дули 2018). Кроз историју, створено је много криптографских система, почевши од Цезара који је шифрирао своје поруке у ратовима, до данас када имамо на стотине развијених криптографских система (Дејвис 1997). Данас су најчешће коришћени системи симетрични и асиметрични шифарски системи, а најпознатији представници су DES (*Data Encryption Standard*) и AES (*Advanced Encryption Standard*) код симетричних, а RSA (*Rivest–Shamir–Adleman*) код асиметричних шифарских система (Виеновић, Адамовић 2013).

Чест математички основ за формирање једног криптографског система су поља Галоа и њихова проширења (Марфи, Робшо 2002; Даемен, Ријмен 2002; Десоки, Асхикмин 2006). Поље Галоа се може дефинисати као „коначно проширење L датог поља K, ако је фиксно поље Галоове групе $\Gamma = G_{L,K}$ управо само поље $K = \Gamma^{\circ}$, то јест ако су елементи из K, и само они, фиксни у односу на сваки K-аутоморфизам $\pi : L \to L$" (Калајџић 2011). Модел коришћен у овом раду заснива се на коначном пољу Галоа GF(2^8), које се најчешће користи код AES система (Марфи, Робшав 2002; Даемен, Ријмен 2002; Десоки, Асхикмин 2006). У оваквим криптографским системима бајт се посматра као елемент бинарног коначног поља дефинисаног несводљивим „Rijndael" полиномом $P(x) = x^8 + x^4 + x^3 + x + 1$ (Марфи, Робшо 2002). Тако формирано поље користи велики број инверзних операција користећи

се аритметиком по модулу 26. На пример, AES користи операцију супротни елемент у односу на множење у пољу GF(2^8) (Десоки, Асхикмин 2006). Такође, у том пољу су имплементиране и операције над полиномима произвољног степена, а коефицијенти су им у опсегу од 0 до 255 из поља GF(2^8) (Даемен, Ријмен 2002). Једна таква операција је и Лагранжова интерполациона формула.

Проблем конструкције непрекидно дефинисане функције из датих дискретних података неизбежан је кад год се жели њима манипулисати на начин који захтева информације које нису експлицитно укључене у податке. Релативно најлакши и у многим апликацијама често најпожељнији приступ решавању проблема је интерполација, где је апроксимациона функција конструисана тако да се савршено слаже са обично непознатом оригиналном функцијом на датим мерним тачкама. У практичној примени коначног рачуна проблема интерполације је следеће: нека су дате вредности функције за коначан скуп аргумената, одредити вредност функције за дати аргумент (Хусиен 2011).

Нека је функција f дата својим вредностима $f_x = f(x_k)$ у тачкама x_k, $(k = 0,1,\ldots,n)$. Не умањујући општост претпоставимо да је:

$$a \le x_0 \le x_1 \le \ldots \le x_k \le b$$

Ако тачке x_k узмемо као интерполационе чворове и ставимо $\varphi_k(x) = x^k$, $(k = 0,1,\ldots,n)$, имамо проблем интерполације функције f алгебарским полиномом. Нека је то полином P_n, тј. (Миловановић 1988):

$$P_n = a_0 + a_1 x + \ldots + a_n x^n$$

Лема: **Лагранжов интерполациони полином** (Ковач, Ковач, Фазекас 2005):

Полином P_n је јединствен и може се представити у облику:

$$P_n(x) = \sum_{k=0}^{n} f(x_k) L_k(x)$$

где је:

$$L_k = \prod_{k,j=0,k\neq k}^{n} \frac{x - x_k}{x_j - x_k}$$

Горепоменуто се сада примењује на криптографске проблеме одлучивања у групи која има, на пример, десет чланова а за добијање кључа потребно је седам делова. За цео број a који је између 0 и 255, генеришу се насумични цели бројеви $r_1, r_2, \ldots, r_6$ у опсегу од 0 до 255. За тако дате вредности формира се полином $f(x)$ над пољем GF(2^8):

$$f(x) = a + r_1 x + \cdots + r_6 x^6$$

Јасно је да је $f(0) = a$. Након тога се рачунају вредности $f(1),\ldots,f(10)$, при чему наведени бројеви представљају елементе поља GF(28) са операцијама у том пољу.

Сада се формирају уређени парови $p_1 = (1, f(1)),\ldots, p_{10} = (10, f(10))$ и имплементира функција која на основу насумичних 7 од 10 парова помоћу Лагранжове интерполационе формуле рачуна $f(0)$, што је заправо вредност a.

Горенаведено се може применити на групу од десет особа која би требало да двотрећинском већином донесе одлуку о извршењу неке радње заштићене кључем. Ако кључ поседује једна или све особе, онда би само једна особа могла да донесе одлуку, што је идентично ситуацији када нема кључа. Са друге стране, ако се кључ подели на десет делова од којих се сваки додели по једној од десет особа у групи, може се десити да, иако се девет чланова групе сложи да се радња изврши, десети власник дела кључа то стопира тако што неће приложити свој део, а то опет не би било пожељно код групног рада. Када је кључ цео број a од 0 до 255, могу се формирати парови $p_1,\ldots,p_{10}$ на описани начин и сваком члану групе доделити један од парова. Уколико било којих седам власника парова одлучи да радња буде извршена, они могу помоћу Лагранжовог интерполационог полинома израчунати a. Међутим, ако се шест или мање особа договори да искористи своје парове, они неће моћи коришћењем Лагранжовог интерполационог полинома добити кључ a, па самим тим неће моћи да изврше жељену радњу. Дакле, кључ a од 0 до 255 може се поделити на десет делова, тако да се помоћу седам од датих десет делова тај кључ може израчунати, док се помоћу мање од седам делова добија погрешан кључ.

Могу се користити било који други бројеви уместо седам и десет. На пример, за 6 чланова групе, тајни цео број би се поделио на 6 делова, а само помоћу најмање четири уређена пара добио би се тајни број a, тј. вредност формираног полинома у тачки 0. Генерисали би се насумични цели бројеви $r_1, r_2,\ldots, r_3$ у опсегу од 0 до 255 и за тако дате вредности формирао би се полином $f(x)$ над пољем GF(2^8):

$$f(x) = a + r_1 x + \cdots + r_3 x^3$$

Затим би се формирали уређени парови $p_1 = (1, f(1)),\ldots, p_6 = (6, f(6))$ који би били додељени члановима групе.

Уколико би о некој радњи одлучивало пет особа, од којих једна има из неког разлога два пута веће право гласа од осталих, на пример најбољи студенти у групи при одлучивању отварања помоћи, онда би кључ био подељен на шест делова, од којих би та особа добила два дела а остале четири особе по један део. За откључавање радње било би потребно четири дела кључа.

ПСЕУДОАЛГОРИТАМ КРИПТОГРАФСКОГ МОДЕЛА

У овом раду развијена је примена поменутог криптографског система коришћењем програмског језика Пајтон. Први корак у писању кода је формирање и имплементација GF(2^8). Над пољем Z_2 има 256 полинома степена 8. Како коефицијент уз x^8 не може бити 0, а у пољу је Z_2, он мора бити 1. Затим се проналазе сви несводљиви полиноми степена 8 и бира један којим ће се извршити просто проширење поља Z_2. Новонастало поље је поље са 256 елемената. Ти елементи се могу представити као цели бројеви од 0 до 255. Имплементирају се операције сабирања и одузимања које су одговарајуће операцијама сабирања и одузимања над одговарајућим полиномима. Може се показати да се у пољу GF(2^8) операције сабирања и одузимања не разликују, тј. да важи да је $x - y = x + y$, где су x и y бројеви од 0 до 255. Затим се имплементира операција множења над целим бројевима од 0 до 255, која одговара операцији множења над одговарајућим полиномима. Помоћу проширеног Еуклидовог алгоритма се налази инверзни елемент у односу на множење. Последњи корак у формирању поља GF(2^8) јесте имплементација дељења. Операција дељења је заправо множење дељеника инверзним елементом који одговара делиоцу, па се ова операција своди на две претходно описане операције.

Као и већина програмских језика, и Пајтон користи библиотеке које олакшавају имплементацију поља GF(2^8). У овом раду коришћена је fieldfinite.py библиотека. Након инсталације библиотеке, она се позива у Пајтону *from pyfinite import ffield*, а затим се формира одговарајуће поље Галоа, у овом случају то је GF(2^8), на следећи начин: *F=ffield.FField(8)*. Функције коришћене из горепоменуте библиотеке, а за потребе овог модела су: сабирање – *F.Add(vrednos1, vrednost2)*, множење – *F.Multiply(vrednost1, vrednost2)* и дељење – *F.Divide(vrednost1, vrednost2)*.

Након формирања и имплементације поља GF(2^8), могу се увести полиноми над тим пољем. Полиноми могу имати произвољан степен, а коефицијенти су им елементи из поља GF(2^8) којих има 256, то јест цели бројеви од 0 до 255. Полиноми над GF(2^8) пољем се у Пајтону могу посматрати као n-торке уређених парова, где први члан пара представља коефицијент полинома, а други члан степен. На пример, полином $P_n(x)$, $x \in \{0,255\}$ се може представити на следећи начин:

$$P_n(x) = ((a_{n-1},\ n-1),(a_{n-2},\ n-2),\ldots,(a_0,0))$$

где су $a_{n-1}, a_{n-2}, \ldots, a_0$ коефицијенти са вредностима из поља GF(2^8), а $n-1, n-2, \ldots, 0$ степени уз промељиву x полинома $P_n(x)$, $x \in \{0,255\}$. На пример, полином $5x^6 + 3x^4 + 9x^2 + 3$ се записује у облику $((5,6),(3,4),(9,2),(3,0))$.

За потребе модела у раду било је потребно имплементирати сабирање и множење полинома, рачунање вредности полинома у тачки, конверзију елемента поља у константан полином и композицију полинома. Поред ових функција, биле су потребне и неке помоћне функције које ће бити објашњене касније у раду.

Алгоритам за сабирање (*addpoly(polinom1, polinom2)*) два полинома упоређује степене променљивих та два полинома. Кроз петљу програм упоређује други члан сваког уређеног пара оба полинома на истим позицијама. Уколико су исти, први чланови се сабирају и тако настали елементи формирају нови полином. Они уређени парови који немају исти други члан при упоређивању се уписују у нови полином у изворном облику. Ако је један од полинома једнак нули, онда се ненула полином преписује (Кнут 1968). Код алгоритма за криптографски модел операције сабирања и множења одговарају операцијама сабирања и множења у пољу GF(2^8).

Множење полинома (*multipoly(polinom1, polinom2))* се извршава тако што се у петљи множи сваки од првих чланова уређених парова једног полинома са првим члановима уређених парова другог полинома, а други чланови се сабирају (Ахо, Хопкрофт 1974). И у овим случају операције су у GF(2^8).

Функција за рачунање полинома у тачки (*vrednost_u_tacki(tačka, polinom)*) израчунава колико износи полином $P(x)$ за неку вредност *b*, тј. рачуна $P(b)$. Са друге стране, функција за конверзију елемента поља у константу (*konverzija(promenljiva)),* променљиву *a* претвара у полином, тј. у облик $(a,0)$.

Ако су дата два полинома $P(x)$ и $Q(x)$, проблем композиције се састоји у проналажењу полинома $P(Q(x))$ (Харт, Новоцин 2011). Стандардне методе подразумевају Хорнеров метод (Кнут 1997), проширени Хорнеров метод (Харт, Новоцин 2011), алгоритам за композицију полинома у Пернаштајновој основи (Де Бор 1987) и алгоритме засноване на процени тачке праћене интерполацијом коефицијента (Пан 2001).

Функција имплементирана у криптографски модел, *kompozicija(polinom1, polinom2)* много је једноставнија од горенаведених и базира се на најједноставнијем математичком методу композиције два полинома. Дакле, за полиноме $P(x)=a_nx^n+\cdots+a_1x+a_0$ и $Q(x)=b_mx^m+\cdots+b_1x+b_0$, функција рачуна композицију на следећи начин:

$$P(Q(X))=a_n(b_mx^m+\cdots+b_1x+b_0)^n+\cdots+a_1(b_mx^m+\cdots+b_1x+b_0)+a_0$$

Због прегледности кода, ова функција је састављена из две једноставније функције. Из претходно написаног лако се уочава да је композиција два полинома заправо замена променљиве првог полинома читавим изразом другог полинома. Ако се то још мало разложи, види се да је то заправо циклично степеновање полинома, а затим множење одговарајућом константом. Дакле,

функције које су учествовале у формирању функције *kompozicija(polinom1, polinom2)* јесу степеновање полинома и множење полинома константом. Степеновање полинома (*stepenovanje_polinoma(polinom,stepen)*) је ракурзивна функција која множи полином самим собом, онолико пута колики је степен (Милутиновић, Ђорђевић 2019). Множење полинома константом (*mnozenje_polinoma_konstantom(konstanta,polinom)*) заправо се своди на правило дистрибутивности, тј. да се сваки члан полинома множи датом променљивом.

Као што је већ наведено у раду, да би криптографски модел могао да штити податке, неопходан је Лагранжов интерполациони полином. Функција је имплементирана на основу формуле у Леми о Лагранжовом интерполационом полиному.

Та функција у Пајтон коду изгледа на следећи начин:

```
def Lagrange (0, (tačka, vrednost_u_tački)):
    Lagranžov_polinom=0
    for k in range ( len(tačka) ):
        t=1
        for j in range ( len(tačka) ):
            if j != k:
                m= F.Add(0, tačka[j])
                n=F.Add(tačka[k], tačka[j])
                if m=0:
                    d=0
                else:
                    d=F.Divide(m,n)
                t=F.Multiply(d,t)
        Lagranžov_polinom=F.Add(F.Multiply(vrednost_u_tački,t),
Lagranžov_polinom)
        return Lagranžov_polinom
```

У датом криптографском моделу, уређени парови (tačka, vrednost_u_tački) прво се упишу у низ, а затим се из тог низа уписују прве, односно друге вредности уређених парова у нове низове. Функције коришћене за то су *razdvajanje_x(polinom)* и *razdvajanje_y(polinom)*. Обе функционишу на сличан начин, и то тако што петљом кроз дужину низа уређених парова читају само први (други) елемент и уписују у нови низ.

Када је имплементиран Лангранжев интерполациони полином, треба одабрати кључ. За одабир кључа *a*, може се користити функција *random* (Кнут 1968) која би насумично одабрала цео број између 0 и 255 или сам корисник може одабрати кључ. Како би професор који поставља систем за заштиту требало да зна кључ, овај модел се заснива на могућности да сам корисник одабере кључ.

У нашем примеру узето је да се кључ дели на десет делова, тј. да група има десет чланова, што значи да о некој радњи одлучује десет особа. Када професор одабере кључ *a*, на пример $a = 13$, формира се полином одређеног степена чији су коефицијенти уз променљиву насумично одабрани цели бројеви од 0 до 225, изабрани коришћењем функције *random*, а чији је слободан члан управо тај кључ. Очигледно, вредност овог полинома у нули једнака

је баш кључу *a*. На основу тог насумично креираног полинома, потребно је пронаћи вредности полинома у тачкама од 1 до 10, што обезбеђује функција *vrednost_polinoma_u_tacki* за рачунање вредности полинома у тачки, а уређени парови који су састављени од дате тачке и вредности полинома у датој тачки представљају делове кључа. На тај начин, професор ствара уређене парове бројева који ће бити додељени студентима да би могли да добију шифру која би им омогућила да откључају одговарајуће информације.

На самом крају, потребно је тестирати да ли модел заиста исправно имплементира принцип 2/3 гласова, тј. да ли се при уносу мање од 2/3 делова кључа добија главни кључ за откључавање одговарајућих података. Функција *test* на основу функција *random.sample* и функције *Lagrange* за Лагранжов интерполациони полином рачуна вредност у нули. Варијација функције *random*, *random.sample* искоришћена је за одабир одређеног броја насумичних парова, тј. делова кључа, што би на неки начин симулирало број ученика из једне групе, који добровољно дају своје делове кључа. Након тога, помоћу тако одабраних парова функција *Lagrange* рачуна вредности кључа *a*. Функција *test* за одговарајући број уређених парова, и то за седам или више парова, требало би да такође израчуна вредност броја *a*. У Табели 1 приказане су вредности за које је функција *test* израчунала вредност кључа на основу одговарајућег броја насумичних парова. Као што је већ речено, унапред одабрана вредност кључа је $a = 13$, а група има 10 чланова.

Табела 1. Вредности добијене функцијом *test*

Број насумичних парова	Насумични парови	Вредност кључа *a*
1	(8, 185)	185
2	(5, 170), (3, 213)	100
3	(1, 16), (3, 213), (8, 185)	152
4	(8, 185), (5, 170), (10, 120), (9, 55)	201
5	(6, 221), (4, 75), (3, 213), (1, 16), (7, 48)	204
6	(6, 221), (9, 55), (5, 170), (7, 48), (1, 16), (4, 75)	203
7	(8, 185), (6, 221), (1, 16), (10, 120), (2, 196), (5, 170), (4, 75)	13
8	(8, 185), (5, 170), (6, 221), (7, 48), (9, 55), (2, 196), (4, 75), (1, 16)	13
9	(4, 75), (1, 16), (9, 55), (10, 120), (3, 213), (6, 221), (5, 170), (2, 196), (7, 48)	13
10	(6, 221), (8, 185), (3, 213), (2, 196), (10, 120), (5, 170), (4, 75), (1, 16), (9, 55), (7, 48)	13

На основу Табеле 1 може се видети да тек када се употреби седам или више делова кључа, функција израчунава одговарајући кључ. Другим речима, тек ако се седам или више особа сложи да се изврши одређена радња, добиће се одговарајући кључ. Овим се може закључити да модел ради исправно, тј. да заиста важи правило двотрећинске већине.

ПРИМЕНА У НАСТАВИ

Као што је већ напоменуто у уводу, криптографија може имати примене у настави кроз заштиту података, помагање у одлучивању у оквиру групног рада, као и многим другим сферама. Приказани модел се може примењивати како на студенте, тако и на ученике основних и средњих школа.

Када је у питању одлучивање у групном раду, примена би се односила на то да професор користи дати модел како би на основу одабране шифре формирао уређене парове који би представљали делове кључа. Сваки од студената у оквиру једне групе добио би по један такав уређен пар. Уколико желе да отворе, тј. погледају одговарајућа упутства или помоћ у решавању задатог проблема, потребно је да најмање две трећине студената од укупног броја чланова групе искористи свој део кључа.

Поменути криптографски модел може се једноставно применити и у организацији диференциране наставе приликом онлајн групног рада, ради добијања „прве", „друге" и „треће" помоћи (Егерић, Милутиновић 2003) при решавању одређеног проблема или задатка који, на пример, носи 10 бодова. Сваки ниво помоћи би био заштићен шифром, а свака од шифара би била подељена на онолико уређених парова колико има студената у групи. Уколико студентима није потребна помоћ и могу сами да реше добијени задатак, они неће искористити уређене парове за добијање кључа, тј. отварање помоћи, и освојиће максималан број бодова.

Ако су им ипак потребна додатна усмерења, уколико се двотрећинском већином договоре, они ће употребити своје уређене парове да добију први кључ и отворити „прву помоћ", која ће их благо усмерити ка решењу датог проблема. Отварање „прве помоћи" ће бити забележено и сви чланови групе изгубиће по 2 бода.

Ако и поред тога не успеју да реше проблем, или знају од самог почетка да им „прва помоћ" неће бити довољна, студенти могу да употребе своје уређене парове другог кључа и тиме отворе „другу помоћ" која би им дала детаљнија упутства и решене примере сличне датом проблему. Уколико би ученици отворили ову помоћ било би им одузето по 5 бодова.

Уколико ни тада не реше проблем, могу искористити и уређене парове за трећи кључ и отворити „трећу помоћ", која садржи опширно упутство и део решења. У том случају би им било одузето 8 бодова. Студенти могу прескочити прве две помоћи и одмах отворити „трећу помоћ", ако су сигурни да немају знања да реше проблем самостално или помоћу упутстава прве две помоћи. Професор проверава коју су последњу помоћ ученици отворили и на основу тога додељује бодове свим члановима групе под условом да су тачно решили задатак. На пример, ако су одмах отворили трећу помоћ, биће им одузето по 8 бодова. Са друге стране ако су отворили и прву и другу помоћ, али не и трећу, биће им одузето по 5 бодова, тј. казнени бодови се не сабирају.

ПРИМЕР ЈЕДНОГ ЗАДАТКА

Нека на решавању једног задатка из предмета Програмирање ради десет студената који похађају изборно предметно подручје из Информатике на Факултету педагошких наука у Јагодини. Студенти су већ савладали основе програмског језика Пајтон, контроле тока програма, гранања и понављања, као и писање најосновније функције. Такође, упознати су са концептом декомпоновања сложенијих проблема на једноставније потпроблеме, знају да дефинишу и употребљавају помоћне функције, као и неке елементарне библиотечке функције. Решавањем задатка студенти би требало да утврде писање функција, њихово позивање у главном програму уз контролу тока програма помоћу гранања, као и коришћење локалних и глобалих променљивих. Студентима се даје задатак и дају се уређени парови помоћу којих, ако се договоре, откључавају одговарајућу помоћ.

Задатак: Написати програм који израчунава збир, разлику, производ и количник два цела броја, тј. симулира рад дипитрона коришћењем функција за израчунавање операција. За сваку операцију написати посебну функцију.

На почетку корисник уноси бројеве, а затим бира жељену операцију. Програм штампа резултат. Уколико корисник не одабере ниједну операцију излази се из програма уз одговарајућу поруку.

Шифра за откључавање „прве помоћи" је *13*, а уређени парови су: *(2, 148)*, *(4, 63)*, *(9, 124)*, *(10, 162)*, *(6, 108)*, *(1, 20)*, *(7, 156)*, *(5, 67)*, *(8, 220)*, *(3, 1)*. Сваки од студената једне групе добија по један пар, а шифра је позната једино наставнику.

„Прва помоћ"

Потребно је написати посебне функције за израчунавање сваке операције, тј. за сабирање, одузимање, множење и дељење два броја коришћењем локалних променљивих. У главном програму, након што корисник унесе два броја и изабере жељену операцију, проверава се његов избор и у зависности од тога позива се одговарајућа функција. У њу се преносе вредности које је корисник унео путем аргумената функције. Када функција израчуна и врати резултат у главни програм, та вредност се штампа.

Шифра за „другу помоћ" је *25*, и поново је позната само наставнику. Сваки од студената добија по један од уређених парова: *(8, 41)*, *(7, 178)*, *(3, 247)*, *(10, 245)*, *(5, 11)*, *(9, 47)*, *(6, 77)*, *(4, 203)*, *(1, 237)*, *(2, 60)*.

„Друга помоћ”

Допунити дати код који може изгледати овако:

```
# funkcija za izračunavanje zbira dva broja
def zbir(br1,br2):
    rezultat = br1 + br2
    return rezultat
    ...          # dopuniti, tj. napisati funkcije za razliku,
proizvod i količnik
""" Glavna funkcija tj. program poziva odgovarajuće funkcije za
izvršavanje tražene operacije """
def digitron():
    prvi = int(input("Unesi prvi broj: "))
    drugi = int(input("Unesi drugi broj: "))
    print("Izaberite racunsku operaciju: (1) Sabiranje, (2)
Oduzimanje, (3) Deljenje, (4) Mnozenje")
    izbor= input()
    ...          # dopuniti if-elif-else izrazom
""" Korišćenjem složenog if-elif-else izraza, odnosno uslovnog
izvršavanja, testirati uslove koji ispituju izbor korisnika. U zavisnosti
od toga koji je uslov zadovoljen poziva se odgovarajuća funkcija i štampa
rezultat. Ukoliko je korisnik uneo drugačiju vrednost od ponuđenih
za izbor računske operacije, izlazi se iz programa uz poruku da nije
izabrana ni jedna operacija.
"""
```

Шифра „треће помоћи” је *139*, позната је само наставнику, а студенти поново добијају по један од следећих уређених парова: *(9, 39)*, *(2, 156)*, *(6, 200)*, *(4, 163)*, *(10, 174)*, *(7, 188)*, *(1, 152)*, *(5, 194)*, *(8, 109)*, *(3, 154)*.

„Трећа помоћ”

Дат је већи део кода који је потребно допунити оним што недостаје:

```
def zbir(br1,br2):
    rezultat = br1 + br2
    return rezultat

...                      # dopisati funkcije koje nedostaju
def proizvod(br1,br2):
    rezultat = br1 * br2
    return rezultat


def digirton():
    print("Pokrenuli ste digitron...")
    print("Unesite brojeve i odaberite racunsku operaciju")
    prvi = int(input("Unesite prvi broj: "))
    drugi = int(input("Unesite drugi broj: "))

    print("Izaberite racunsku operaciju: ((1) Sabiranje, (2)
Oduzimanje, (3) Deljenje, (4) Mnozenje")
    izbor= input()
    if izbor == "1":
          print("Rezultat je",zbir(prvi,drugi))
       ...             # dopuniti

    elif izbor == "4":
          print ("Rezultat je",proizvod(prvi,drugi))
    else:
         print("Niste izabrali nijednu operaciju. Hvala sto ste
koristili digitron")
```

На овај начин студенти самостално одређују да ли им је потребна помоћ и у којој мери, без интервенције наставника. Студенти би добијали мали извршни фајл помоћу кога би могли открити шифру под којом је закључана помоћ, а сама помоћ би се налазила на Мудл платформи која нуди могућност закључавања података, као и бележење приступа датим подацима. Стога, групни рад би могао у потпуности бити организован онлајн.

ЗАКЉУЧАК

Због тренутне ситуације услед пандемије ковида 19, али и све веће потребе да се део учења преусмери на онлајн-рад, потребно је обезбедити како заштиту одговарајућих података, тако и добру организацију која би студентима омогућила да уз договор са другима одаберу када и под којим условима ће добити одговарајуће помоћне информације. Велики број образовних установа користи Мудл платформу као систем за управљање онлајн-учењем, што подразумева, поред дељења информација, комуникацију, организовање групног рада итд., али и могућност шифровања и закључавања информација. Ако би се студентима, члановима једне групе дале шифре, онда би у оквиру те групе појединци могли отворити одговарајуће информације и без пристанка осталих чланова групе, што би требало спречити. Коришћењем криптографских решења, чланови једне групе би тек пошто се више од две трећине њих сложи, могли отворити одговарајућу помоћ за израду задужења. Договор је потребно постићи јер са једне стране помаже у изради задатка а са друге стране доводи до смањења освојених бодова. То значи да би требало тек након међусобне сарадње чланова групе, размене идеја и мишљења, отворити неки ниво помоћи само ако се већина сложи да другачије не могу доћи до решења проблема.

Поред могућности лакшег договора и одлука у оквиру група, овакав начин рада би смањио и оптерећење наставника, јер не би морао да надгледа читав процес решавања датог проблема, нити да сам даје упутства и одлучује о смањивању бодова. Са друге стране, смањује се субјективност у оцењивању рада студената.

Овај модел се може применити на било ком наставном предмету и било ком нивоу образовања, што обезбеђује широку примену у настави, чиме би биле умањене шансе за преписивање и преваре у израдама групних радова и пројеката.

ЛИТЕРАТУРА

Ахо, Хопкрофт (1974): A. Aho, J. Hopcroft, *The Design and Analysis of Computer Algorithms*, Massachusetts: Addison-Wesley Longman.

Ален, Симен (2008): E. Allen, J. Seaman, *Staying the course: Online education in the United States*, Sloan Consortium, PO Box 1238, Newburyport, MA 01950.

Ален, Боурхис, Барел, Марбри (2002): M. Allen, J. Bourhis, N. Burrell, E. Marbry, Comparing Student Satisfaction With Distance Education to Traditional Classrooms in Higher Education: A Meta-Analysis, *American Journal of Distance Education*, 16(2*)*, 83–97.

Арготе, Груенфелд, Накуин (2001): L. Argote, D. H. Gruenfeld, C. Naquin, Group learning in organizations, In: M. E. Turner (Ed.), *Groups atwork: Advances in theory and research*, Mahwah, NJ: Lawrence Erlbaum Associates, 369–411.

Бејти, Уласевиц (2006): B. Beatty, C. Ulasewicz, Faculty perspectives on moving from Blackboard to the Moodle learning management system, *TechTrends*, 50(4), 36–45.

Костело (2013): E. Costello, Opening up to open source: Looking at how Moodle was adopted in higher education, *Open Learning: The Journal of Open, Distance and e-Learning*, 28(3), 187–200.

Даемен, Ријмен (2002): J. Daemen, V. Rijmen, *The Design of Rijndael – AES – The Advanced Encryption Standard*, Berlin: Springer-Verlag.

Дејвис (1997): D. Davies, A brief history of cryptography, *Information Security Technical Report*, 2(2), 14–17.

Де Бор (1987): C. de Boor, *B-form basics*, Wisconsin univ – Madison Mathematics Research Center.

Десоки, Асхикмин (2006): A. Desoky, A. Ashikhmin, Cryptography Software System using Galois Field Arithmetic, *2006 IEEE Information Assurance Workshop*, West Point, NY: IEEE, 386–387.

Дојумгач, Танхан, Кимаз (2020): İ. Doyumğaç, A. Tanhan, M. S. Kiymaz, Understanding the Most Important Facilitators and Barriers for Online Education during COVID-19 through Online Photovoice Methodology, *International Journal of Higher Education*, 10(1), 166–190.

Дули (2008): J. F. Dooley, *History of cryptography and cryptanalysis: Codes, Ciphers, and their algorithms*, Springer.

Ескобар-Родригез, Монж-Лозано (2012): T. Escobar-Rodriguez, P. Monge-Lozano, The acceptance of Moodle technology by business administration students, *Computers & Education*, 58(4), 1085–1093.

Харт, Новоцин (2011): W. Hart, A. Novocin, Practical Divide-and-Conquer Algorithms for Polynomial Arithmetic, In: V. P. Gerdt, W. Koepf, E. W. Mayr, E.V. Vorozhtsov (Eds.), *Computer Algebra in Scientific Computing. CASC 2011. Lecture Notes in Computer Science*, vol 6885, Berlin, Heidelberg: Springer.

Хусиен (2011): K. A. Hussien, The Lagrange Interpolation Polynomial for Neural Network Learning, *International Journal of Computer Science and Network Security*, 11(3), 255–261.

Калајџић (2011): G. Kalajdžić, *Algebra*, Beograd: Zavod za udžbenike.

Кнут (1968): D. Knuth, *The Art of Computer Programming, Volume 1: Fundamental Algorithms*, Massachusetts: Addison Wesley Longman.

Кнут (1997): D. Knuth, *The Art of Computer Programming, volume 2: Seminumerical Algorithms*, Massachusetts: Addison-Wesley.

Коцака, Бозана, Иуика (2009): Z. Koçaka, R. Bozana, Ö. Iúıka, The importance of group work in mathematics, *Procedia Social and Behavioral Sciences 1*, 2363–2365.

Ковач, Ковач, Фазекас (2005): A. Kovács, L. Kovács, F. Fazekas, The Lagrange Interpolation Formula in Determining the Fluid's Velocity Potential through Profile Grids, *Semantic Scholar*, 26–29.

Ли (2010): J.-W. Lee, Online support service quality, online learning acceptance, and student satisfaction, *Internet and Higher Education*, 13, 277–283.

Лаки, Бранам, Етчисон (2019): A. Lucky, M. Branham, R. Atchison, Collection-Based Education by Distance and Face to Face: Learning Outcomes and Academic Dishonesty, *Journal of Science Education and Technology*, 28(1), 414–428.

Миловановић (1988): G. Milovanović, *Numerička analiza II deo*, Beograd: Naučna knjiga.

Милутиновић, Ђорђевић (2019): В. Милутиновић, С. Ђорђевић, *Програмирање у Пајтону са задацима за вежбање*, Јагодина: Факултет педагошких наука Универзитета у Крагујевцу.

Марфи, Робшо (2002): S. Murphy, M. J. Robshaw, Essential Algebraic Structure within the AES, *Annual International Cryptology Conference*, Berlin, Heidelberg: Springer, 1–16.

Пан (2001): V. Pan, *Structured matrices and polynomials: unified superfast algorithms*, New York: Springer-Verlag.

Танхан (2020): A. Tanhan, Utilizing online photovoice (OPV) methodology to address biopsychosocial spiritual economic issues and wellbeing during COVID-19: Adapting OPV to Turkish, *Turkish Studies*,15(4), 1029–1086.

Виеновић, Адамовић (2013): M. Vienović, S. Adamović, *Kriptologija I – Osnove za analizu i sintezu šifarskih sistema*, Beograd: Univerzitet Singidunum.

Егерић, Милутиновић (2003): М. Егерић, В. Милутиновић, Решавање проблемских задатака уз помоћ компјутера, *Зборник радова*, 7, 293–301. ISSN 0354-9895

Suzana M. Đorđević

Verica R. Milutinović

University of Kragujevac
Faculty of Education in Jagodina
Department of Mathematics and Informatics

APPLICATION OF DATA PROTECTION CRYPTOGRAPHIC MODEL IN STUDENT GROUP WORK

Summary: The aim of this study is to present a data protection cryptographic model which can assist students in making decisions within group work. Using group work in assessing students has been increasing recently, due to the growing use of the Internet in teaching, especially during the COVID-19 pandemic which made group work shift to the online form. In order to prevent possible copying and disagreements between group members, it is necessary to develop a system that will protect data, but also allow group members to reach an agreement in a voluntary, solidary and democratic way. One of the possible solutions is the use of cryptography. For the purpose of developing a cryptographic model,

Galois fields GF(256) were used and mathematical operations in the polynomial field in GF(256) were developed. The Lagrange interpolation polynomial is then implemented in the model, which allows the teacher to generate ordered pairs that are part of the key. In this paper, such a model is developed and a pseudo algorithm for the given model is presented. In addition, an example of application of the model in teaching programming is given.

Keywords: cryptography, Galois fields, Lagrange interpolation polynomial, teaching programming, group work.