NDËRTIMI I SHEMBUJVE TË FORTË E DIAGNOSTIKË NË MASSEY – OMURA DHE EMO1 MBI FUSHA TË FUNDME DHE MBI VIJA ELIPTIKE

***HYKA D., BAXHAKU A.**

Universiteti i Tiranës, Fakulteti i Shkencave të Natyrës, Departamenti i Matematikës

e-mail: dolantina.hyka@fshn.edu.al

Përmbledhje

Në të paraqitet një algoritëm për gjenerimin e shembujve të fortë ose diagnostikë për kriptosistemin Massey – Omura mbi vijat eliptike. Synimi është ndërtimi i algoritmeve që ndërtojnë shembuj me parametra të tillë që të shmangin gabimet e padiktuara dhe/ose të dallojnë llojin e gabimit të kryer gjatë ekzekutimit të algoritmit kriptografik të konsideruar. Për këtë konsiderohen fillimisht gabimet e mundshme që mund të kryen në llogaritjet e hapave të algoritmit kriptografik, e më pas synohet ndërtimi i një e një algoritmi që gjeneron shembuj me parametra të cilët shmangin të gjithë gabimet e trajtuara analitikisht. Ideja e kësaj metode mund të përdoret jo vetëm në kriptografi, por edhe në mjaft disiplina të tjera matematikore, ekonomike, fizike, informatike, etj.

Abstract

An algorithm for generating strong/diagnostic cryptographic examples relating with Elliptic Curves is presented. The main goal is avoiding the "undetected errors" during the implementation of any considered crytposystem, which bring to right answers even if any wrong method is followed. The possible "undetected errors" are selected and then isolated by constructing an algorithm generating examples being strong or diagnostic ones depending on the chosen parameters.The idea used may be applied even in other disciplines, mathematical or non-mathematical ones, p.es. differential equations, matrix algebra, financial mathematics, micro-economy, finance, physics, etc.

Fjalëkyçe: shembuj të fortë / diagnostikë, Kriptografia me çelës publik, EMO1, EMO2, ECC.

Hyrje

Kriptografia tashmë është pjesë e programeve mësimorë si lëndë e veçantë, veçanërisht në degët matematikë, informatikë, teknologji informacioni, elektronikë, ekonomik, etj. Në këto degë ajo ndikim të drejtpërdrejtë, duke ndikuar në pajisjen e studentëve me kulturën dhe aftësitë e nevojshme për të kuptuar, përdorur apo dhe ndërtuar programe dhe protokolle kriptografikë të zbatuar në kompjuterë, telefona, radiomarrëse, karta krediti apo debiti e në shumë aparatura të tjera të cilat mund të shërbejnë si aparatura përgjimi apo të mbrojtjes së të dhënave personale (*privacy*), në sigurinë e firmave ose të bankave e deri tek siguria shtetërore.

Në këtë material paraqiten disa algoritma të cilët gjenerojnë shembuj të fortë kriptografikë dhe shembuj diagnostikë lidhur me kriptosistemin *Massey – Omura* mbi $'_p$, *EMO1* mbi $'_n$ dhe *Massey- Omura* mbi vijat eliptike. Skema e ndjekur për ndërtimin e tyre është si më poshtë:

Fillimisht janë paraqitur në mënyrë analitike algoritmet e shifrimit e të deshifrimit për kriptosistemet e shqyrtuara, janë dalluar kandidatët për gabime të padiktuara që mund të bëhen gjatë ndërtimit të shembujve si edhe mënyra e shmangies për secilin prej këtyre gabimeve. Pasi parashtrohet problemi dhe jepen mënyrat se si duhen ndërtuar shembujt për të shmangur secilin nga këto gabime, paraqitet edhe algoritmi i përbashkët, i realizuar në Maple. Me anë të ekzekutimit të këtij algoritmi, gjenerohen shembuj të fortë e shembuj diagnostikë në varësi të programit të ndërtuar.

1. Massey – Omura në fushat e fundme $'_p$ (Chong, 2003)

Qëllimi është gjenerimi i parametrave të shembujve të një primitive kriptografikë të tillë që të evidentojnë zbatime të gabuara të algoritmit duke evituar përftimin e rezultateve të sakta në secilin nga ato zbatime.

Trajtimi nën këtë këndvështrim të përgjithshëm kërkon studimin deri në imtësi të individualiteve të primitivave kriptografikë në shqyrtim (Hyka, & Baxhaku, 2013, Chong , *et al*. 2006)

Kështu, për kriptosistemin Masey-Omura, si kritere bazë janë veçuar:

I) Algoritmi i shifrimit kryet mbi një fushë të fundme $'_p$ me karakteristikë *p* relativisht të madhe;

II) Si çelësa privatë duhen zgjedhur:

1. $(u,p-1)=1$ pra çelësi *u* duhet të jetë reciprokisht i thjeshtë me $\varphi(p)$ në mënyrë që për vlerën e zgjedhur të çelësit *u* të ekzistojë elementi i anasjelltë *v*. (Chong , *et al*. 2006)

2. $u \neq v$. Nëse çelësi i shifrimit *u* do të ishte i njëjtë me çelësin (e deshifrimit) *v* atëherë do të mund të merrej përfundimi i drejtë duke ekzekutuar algoritmin dhe pa kaluar nga gjetja e elementit të anasjelltë.

3. $u \neq r$. Çelësat e shifrimit të palëve komunikuese duhet të jenë të ndryshme sepse përndryshe edhe çelësat e deshifrimit do ishin të njëjtë, meqë veprimet kryen në të njëjtën fushë. Zgjedhja rastësore e çelësave të njëjtë jo vetëm ul ndjeshëm entropinë e hapësirës së çelësave por dhe rrit gjithashtu ndjeshëm mundësinë e transmetimit të tekstit të hapur në vend të atij të shifruar. Nëse marrësi e shifron gabimisht mesazhin me çelësin e tij *s* në vend të çelësit *r* atëherë ai transmeton tekstin e hapur në vend të

atij të shifruar. Gjithashtu nëse çelësat *u* dhe *r* zgjidhen të njëjtë, studentit mund ti krijohet ideja që M-O vepron vetëm nga njëra palë komunikuese dhe tjetra merret pothuajse inekzistente.

4. $u \neq s$. Arsyetimi është i ngjashëm me rastin e pikës 3.

$(r,p-1)=1$. Gjithashtu çelësi *r* duhet të jetë reciprokisht i thjeshtë me $\varphi(p)$ në mënyrë që për vlerën e zgjedhur të çelësit *r* të ekzistojë elementi i anasjelltë *s*.(Menezes *et al*., 1997)

5. $r \neq s$. Arsyetimi kryhet njësoj si në rastin *2*.
6. $s \neq v$. Edhe në këtë rast vlen arsyetimi i rastit *3*.

III) Veprimet për gjetjen e elementit te anasjelltë duhen kryer sipas modulit *p-1* dhe jo *p*.

Disa nga devijimet e zakonshme nga aplikimi i drejtë i algoritmit:

a) Njehsimi i M_1 , M_2, M_3, M_4 $mod\ (p-1)$ në vend të *mod p*;
b) Gjendet *v, s mod p* në vend të *mod p – 1*;
c) Merret i kundërti i *u, r* në vend të elementit të anasjelltë *v, s* përkatësisht;
d) Ngatërrohet karakteristika e fushës me çelësin privat gjatë llogaritjes së elementit të anasjelltë përkatës (pra në vend që të gjendet $v \ mod\ (p-1)$ [$s \ mod\ (p-1)$], njehsohet $(p-1)^{-1} \ mod\ u$ [$(p-1)^{-1} \ mod\ r$] [9];
e) Përdoret *u* në vend të *v* (*s* në vend të *r*).

Një pjesë e tipit të këtyre gabimeve është trajtuar tek (Chong, et al.,2006), por për mjedise të tjerë.

Tek (Hyka, 2013) është paraqitur një algoritëm i ekzekutueshëm në Maple i cili i shmang këto gabime për rastin e kriptosistemit Massey – Omura mbi $\mathbb{Z}'_p$.

Për të shmangur ndërhyrjen e përgjuesit Eve që në hapin e parë të komunikimit ndërmjet *Alice* dhe *Bob*, mund të përdorim edhe një përmirësim të kriptosistemit *Massey – Omura*, *EMO1* ose *EMO2* (Winton, 2007) Ky i fundit më tepër se një përmirësim mund të shihet edhe si një veprim i njëkohshëm i *EMO1* dhe kriptosistemit *RSA*. Në thelb ka përzgjedhjen e një çelësi publik jo të thjeshtë pra të paraqitet si prodhim *2* ose më shumë numrave të thjeshtë. Dhe me pas të ndiqen hapat e kriptosistemit *Massey – Omura*.

IV) EMO-1 në fusha të fundme $\mathbb{Z}'_n$

Paraqesim fillimisht strukturën e algoritmit të *EMO-1*(Winton., 2007). Përmirësimi që i bëhet algoritmit të kriptosistemit në këtë rast është ndryshimi i fushës në të cilën kryhen veprimet. Një dobësi e njohur e kriptosistemit *Massey – Omura* është se mund të thyhej në hapin e parë për shkak se veprimet kryhen në një fushë të njohur $'_p$. Për rrjedhojë, jo vetëm që kriptosistemi është i epshëm ndaj "sulmeve me njeri ndërmjet", por është gjithashtu i hapur ndaj një sulmi që në një farë mënyre arrin të gjejë çelësin privat të një dërguesi.

Arsyetimi tek (Winton, 2007) është që, nëse në vend të fushës $'_p$ zgjedhim një unazë prodhim kartezian $'_p \times '_q$; $'_{pq} = '_n$, atëherë kundërshtari që ka gjetur një çelës privat do të përballej me problemin e faktorizimit të numrave në prodhim dy faktorësh të thjeshtë, problem mbi të cilin bazohet edhe siguria e kriptosistemit *RShA*. Vështirësia në faktorizimin e modulit të përbashkët *n* çon në rritjen e sigurisë për kriptosistemin dhe për faktin se në këtë mënyrë suksesi i sulmeve me njeri ndërmjet bëhet shumë më i vështirë. Vetëm palët legjitime e njohin çelësat privatë dhe vetëm qendra e autorizuar njeh zbërthimin në faktorë të thjeshtë të *n*-së. Megjithatë ky përmirësim ka dhe aspektet e tij negative pasi duhet marrë parasysh që rritet numri i veprimeve dhe koha e transmetimit të të dhënave.

2.Funksionimi i EMO-1 (Winton, 2007**)**

- *Alice* dhe *Bob* bien dakord për zgjedhjen e një çelësi publik *n* të tillë që $n=pq$ ku *p* e *q* janë numra të thjeshtë.
- Secili prej tyre gjeneron nga një çelës privat *u* – çelësi privat i *Alice*, *r* – çelësi privat i *Bob* të tillë që $(u, \varphi(n))=1$ dhe $(r, \varphi(n))=1$.
- Secili prej tyre mund të njehsojë përkatësisht $v=u^{-1} \bmod \varphi(n)$ dhe $s=r^{-1} \bmod \varphi(n)$.[2)]
- Alice fillimisht konverton mesazhin nga alfanumerik në mesazh numerik $M<n$, më pas llogarit $M_1=M^u \bmod n$ dhe ja dërgon atë *Bob*-it,
- *Bob* e shifron edhe me çelësin e tij mesazhin M_1 duke ndërtuar kështu mesazhin $M_2=M_1^r \bmod n = M^{ur} \bmod n$ dhe ja rikthen *Alice*-s.
- Alice përfton mesazhin $M_3 \equiv M_2^v \equiv M^{urv} \equiv M^r \bmod n$ duke ja ridërguar *Bob*-it.
- Për të lexuar mesazhin ai mjafton të veprojë me çelësin *s* mbi mesazhin e marrë $M \equiv M_3^s \equiv M_2^{rs} \equiv M \bmod n$.

Me gjithë pamjen e ngjashme me kriptosistemin *Massey-Omura*, përmirësimi i arritur me algoritmin kriptografik *EMO-1* në rritjen e sigurisë së tij është i ndjeshëm.

Për ndërtimin e shembujve të fortë kriptografikë ose i shembujve diagnostikë vërejmë se vlejnë të gjitha rastet e shqyrtuara në algoritmin e kriptosistemit *Massey – Omura* duke zëvendësuar përkatësisht *p* me *n* dhe *p-1* me *φ(n)*.

I) Algoritmi i shifrimit kryhet sipas modulit *n=pq*.

II) Si çelësa privatë duhen zgjedhur

1. $(u,\varphi(n))=1$
2. $u\neq v$
3. $u\neq r$
4. $u\neq s$
5. $(r,\varphi(n))=1$
6. $r\neq s$
7. $s\neq v$
8. $v=u^{-1}\bmod\varphi(n)\neq u^{-1}\bmod(n-1)$
9. $s=r^{-1}\bmod\varphi(n)\neq r^{-1}\bmod(n-1)$

Ia vlen të theksohet për *EMO-1* (8,9) është se duhet pasur kujdes që vlera e *v* dhe *s* sipas modulit $\varphi(n)$ nuk duhet të jetë e njëjtë me vlerën e llogaritur sipas modulit *n-1* pasi kështu nuk mund të kontrollojmë rastin kur nuk llogaritet $\varphi(n)=\varphi(p\cdot q)=\varphi(p)\cdot\varphi(q)$ por llogaritet njëlloj sikur *n* të ishte numër i thjeshtë duke cenuar kushtet e algoritmit.

Gjithashtu duhet shmangur rasti (8,9) kur veprimet për gjetjen e elementeve të anasjelltë mund të kryhen sipas modulit *n* në vend të modulit $\varphi(n)$.

Tek (Hyka 2013) është paraqitur një trajtim i ndërtimit të këtyre çelësave dhe një algoritmi përkatës në *Maple* i cili i shmang këto gabime për rastin e përmirësimit të parë të kriptosistemit *Massey – Omura* (*EMO-1*).

3. Kriptosistemi massey – omura mbi vijat eliptike

- *Alice* dhe *Bob* bien dakord të përdorin një vijë eliptike *E* mbi një fushë të fundme F_q [3)] të tillë që problemi i logaritmit diskret të jetë i patrajtueshëm (tepër i vështirë për tu zgjidhur) në të. Fusha e zgjedhur bëhet publike. Le të jetë *p* numri i pikave të vijës eliptike $E(F_q)$.
- Secila nga palët zgjedh në mënyrë të rastit numrat e plotë *u* dhe *r* sipas modulit *p* të tillë që *(u,p-1)=1* dhe *(r,p-1)=1*.
- Llogarisin elementet e anasjelltë përkatës $v=u^{-1}mod(p-1)$ dhe $s=r^{-1}mod(p-1)$.
- Kur *Alice* do t'i çojë *Bob*-it një mesazh *M*, fillimisht ajo duhet ta kthejë mesazhin nga alfanumerik në pika të vijës eliptike të zgjedhur, llogarit $M_1=uM$ (në *E*) dhe ja dërgon mesazhin M_1 palës tjetër.
- Pa tentuar të kontrollojë nëse mund ta kuptojë apo jo mesazhin, *Bob* shumëfishon pikat e vijës eliptike të marra nga *Alice* me anë të çelësit

të tij privat *r* dhe i kthen *Alice* mesazhin $M_2=rM_1$ (në *E*).

- Hapi i tretë është që *Alice* të zbulojë pjesën e shifrimit që i përket asaj duke shumëfishuar pikat e mesazhit M_2 me elementin e anasjelltë *v*. Ajo llogarit mesazhin $M_3= vM_2$ (në *E*) e ja dërgon sërish *Bob*-it.
- Ky i fundit mjafton t'i shumëzojë të gjitha pikat që përmban M_3 me çelësin e tij *r* dhe pasi ti kthejë ato nga pika të vijës eliptike në tekst alfanumerik mund ta lexojë mesazhin.

Për të bërë të mundur ndërtimin e shembujve të fortë kriptografikë ose të shembujve diagnostikë, gjatë hapave të shifrimit e deshifrimit të mesazhit është pasur parasysh që:

Llogaritjet për mesazhet $M_1 - M_4$ mund të kryhen si në rastin e kriptosistemit *Massey – Omura* mbi fushat e fundme $\mathbb{Z}_p$ dhe jo si shumëfishime të pikave që i përkasin një vije eliptike;

Për sa i përket çelësave duhen shmangur të njëjtat gabime si tek *M-O* mbi $\mathbb{Z}_p$ ose në rastin kur vija eliptike është ndërtuar mbi një fushë F_p^n njëlloj si rasti i ndërtimit të çelësave të *EMO-1* ose *EMO-2* (Hyka *et al*. (2013)).

Në ndërtimin e çelësave gjithashtu duhet pasur kujdes në gjetjen e elementit të anasjelltë:

Mund të gjenden elementet e anasjelltë:

$* v=p^{-1}mod(u-1)$ $* v=p^{-1}mod(\varphi(u))$ $* s=p^{-1}mod(r-1)$ $* s=p^{-1}mod(\varphi(r))$

Rezultati i njëjtë në rastin kur pikat e vijës shumëzohen me çelësat përkatës si prodhim me skalar $u(x,y)=(ux,uy)$ ose $(x,y)u=(xu,yu)$ me atë të saktin ku pikat mblidhen sipas algoritmit përkatës në vija eliptike çon në një tjetër gabim për tu evituar pasi studenti në këtë rast nuk përdor fare veprimet mbi vijat eliptike.

Vërejmë që një element i rëndësishëm në procesin e dallimit të gabimeve është zgjedhja e vijës eliptike, për vetë vështirësitë e kodimit të elementeve të mesazhit si pika në një vije eliptike çfarëdo. Nëse mesazhi nuk mund të shprehet si pikë e vijës përkatëse të zgjedhur atëherë ose ndërrojmë vijën eliptike ose ndërrojmë funksionin kodues fillestar. Prandaj një ndër pjesët e algoritmit gjenerues duhet të kontrollojë nëse mesazhi që merret në shqyrtim mundet të kodohet si pikë e vijës eliptike të zgjedhur.

Në vazhdim paraqiten hapat e ndërtimit të algoritmit në Maple i cili i shmang këto gabime për rastin e kriptosistemit Massey – Omura mbi vijat Eliptike.

- Zgjidhet një fushë e fundme.
- Zgjidhet një vijë eliptike mbi atë fushë.

- Konvertohet teksti në pikë të vijës eliptike me anë të një funksioni shifrimi ose të një hash funksioni.
- Zgjidhen çelësat *u,r* që plotësojnë kushtet e trajtuara më sipër.
- Vendosen kushtet për kriptosistemin dhe çelësat si edhe komentet përkatëse për secilin rast të gabimeve në mënyrë që të gjenerohen shembuj ose ushtrime diagnostikë.
- Çelësat konvertohen në sistem binar për të zbatuar më pas algoritmin mbledhje dyfishim lidhur me shumëfishimin e pikave të vijës eliptike.
- Vendosen kushtet për pikat e vijës eliptike ndër të cilat kërkohet edhe që vlerat e shumëfishimit si vektor të jenë të ndryshme nga vlerat e shumëfishimit si pika të vijës përkatëse.

Algoritmi i testuar në *Maple 17* me të dhëna të rendit 2^6(si shembull-lojë) mori një kohe prej 2.5" në një kompjuter Intel (R) Core (TM) i5 CPU 750 @ 2.67GHz RAM 4.00GB OS 32 – bit

Konkluzione

Ndërtimi i sistemeve të fortë ose diagnostikë kriptografikë, ka një rëndësi të veçantë jo vetëm në mësimdhënien e kriptografisë, por edhe në konceptimin dhe krijimin e kriptosistemeve të reja. Me anë të këtyre sistemeve tentohet të shmangen e të evidentohen sa më shumë nga gabimet e mundshme. Prandaj mund të jenë shtysë për të shmangur edhe sulmet e mundshme e për përmirësimin e kriptosistemeve të njohur ose krijimin e atyre të reja.

E njëjta linjë arsyetimi mund të zbatohet edhe në disiplinat e tjera matematikore apo jo të tilla, për të lehtësuar mësimdhënien si edhe për të arritur një vlerësim sa më efektiv e të saktë brenda kufijve kohorë dhe sasiorë.

Literatura

Hyka D. (2013): An overview on diagnostically cryptographic examples IWBCMS

Hyka D., Baxhaku A. (2013): Some maple algorithms generating diagnostically /strong cryptographic examples; ISTI

Hyka D., Baxhaku A. (2013): Generating "sound" cryptographyc examples using different softwares. 5th International Scientific Conference "Economic Policy and EU Integration"

Chong S.K., Farr G., Frost L., Hawley S. (2006): On pedagogically sound examples in public-key cryptography, ACSC

Chong, S. K. (2003): Cryptographic teaching tools, BCompScHonours, Monash University, Clayton, Australia

Winton R., (2007): Enhancing the Massey-Omura Cryptosystem, Journal of Mathematical Sciences & Mathematics Education Vol. 2, No. 1, Feb.

Menezes A., van Oorschot P., Vanstone S., (1997): Handbook of Applied Cryptography", CRC Press,

Koblitz N. (1994): A Course in Number Theory and Cryptography, Springer-Verlag

[1)] Njihet dhe si "protokolli me tre kalime i Shamirit".

[2)] Këtë procedurë mund ta kryejë dhe një *qendër e autorizuar e besuar*, që, mbasi zgjedh faktorët e thjeshtë *p* e *q*, u tregon pjesëmarrësve në skemë (që mund të jenë më shumë se 2), çelësin publik $n=pq$, si dhe nga një çift çelësash shifrimi-deshifrimi $(e,d=e^{-1} mod\ (p-1)(q-1))$ për secilin nga pjesëmarrësit. Skema e paraqitur është e thjeshtuar në rastin e dy pjesëmarësve.

[3)] Në ndërtimin e shembujve është zgjedhur fusha $'_p$, për *p* të thjeshtë.