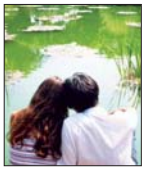
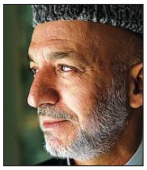
NDRYSHE

Kriptografi
Si ruhen të fshehtat në kohën tonë
NE FAQET 14-15

Dilema
A ekziston gruaja e përsosur...?
NE FAQEN 19



Hamit Karzai:
Marrëveshjet e pista, të domosdoshme
NE FAQEN 20



TOP CHANNEL

Shqip

illy

Drejtor BESNIK MYFTARI
Kryeredaktor URIM BAJRAMI

Viti III - Nr. 152 (802) Emërkurë, 4 qershor 2008 E përditshme e pavarur Çmimi 50 lekë, 1.5 euro

Adresa e redaksisë:
Rr. Sami Frashëri,
Pallatet e Aviacionit, Nr. 4
Tel: 04 2 272 565 • 068(9) 20 35 300
E-mail: info@gazeta-shqip.com
www.gazeta-shqip.com

Dhjetëra fashikuj tërhiqen nga arkivi i Prokurorisë së Tiranës. Hetuesit: "Kemi fakte të reja". Dyshime për motivet e ekzekutimit: Ndoshta politike

Vrasja e Azem Hajdarit, rihapet dosja

Krimi i Organizuar riheton çështjen. Ish-truproja i Berishës pranon të bashkëpunojë

Vrasja e deputetit të Partisë Demokratike, Azem Hajdari, më 12 shtator të vitit 1998, e cilësuar si "vrasja e shekullit", del nga arkivi i Prokurorisë së Tiranës dhe përfundon në zyrën e Kryeprokurores Ina Rama. Dy ditë më parë...
NE FAQET 2-3

Janë ngritur në mënyrë të paligjshme
Gjykata vendos: Të sekuestrohen pronat e Aldo Bares
NE FAQEN 11

Prifti, sekser i shërbimeve funerale
Kisha në krizë financiare, cakton çmime për shërbesat
NE FAQEN 23

ZGJEDHJET QE NUK ZGJIDHEN ASGJE

GEZIM PODGORICA

Megjithëse të imponuara nga shqiptarët, zgjedhjet e parakohshme në Maqedoni, që u iniciuan për të ndryshuar pozitën e tyre dhe për të realizuar një avancim të kërkesave bazike e legjitime, nuk zgjidhën asgjë. Përkundrazi, ato i rënduan problemet dhe i avantazhuan maqedonasit, si në argumentet përballë faktorit ndërkombëtar, ashtu edhe në raportet me partnerin shqiptar...
NE FAQEN 9

DY HERE (MOS ME) KEQ!

MONIKA SHOSHORI STAFA

Edhe pse Komisioni Qendror i Zgjedhjeve në Shkup mund të shpallë një rezultat; megjithëse zyrat e përfaqësive ndërkombëtare mund të pajtohen në heshtje me çka ndodhi; të dielën Maqedonia shënjoi një hap tjetër prapa. Ishte shumë vonë për thirrjen e Presidentit maqedonas Crvenkovski "stabiliteti para procesit". Dështimi i zgjedhjeve politike në Maqedoni, për të gjithë ata që e ndjekin politikën jo si amatorë, por si vëzhgues...
NE FAQEN 9

"Gërdeci", Kryeparlamentarja i shkruan Ina Ramës: Na sill dokumentet për ushtarakët. SHBA: Stop presionit

Topalli mbron Mediun, akuzon Shtabin

Kryetarja e Kuvendit, Jozefina Topalli, i ka nisur dje një letër zyrtare Kryeprokurores Ina Rama, në të cilën merr hapur në mbrojtje ish-ministrin e Mbrojtjes, Fatmir Mediun, dhe sulmon Shtabin e Përgjithshëm të Ushtrisë. Në letrën prej tri faqesh, me numër protokolli 1990, datë 03.06.2008, kreu i legjislativit...
NE FAQEN 5

"Të shqyrtohen brenda datës 9"
PS, ultimatum Topallit. I cakton datat për dy çështje
NE FAQEN 6

Reagon Komiteti për Kushtetutën
"Presioni ndaj Topit, produkt i ndryshimeve kushtetuese"
NE FAQEN 4

Ekonomi

KESH, në garë 4 nga 8 kompani
Privatizimi, "tkurret" interesimi

Nis zyrtarisht shqyrtimi i kompanive që kanë shfaqur interes për të blerë shumicën e aksioneve të Operatorit të Sistemit të Shpërndarjes (OSS) në KESH. Ministria e Ekonomisë, Tregtisë dhe Energjetikës (METE) ka zbardhur emrat konkretë të kompanive të huaja që kishin dorëzuar në ministri...
NE FAQEN 24

Shqiptarët, konsumatorë ilaçesh
Barnat, një biznes miliardash

Pjesa e të ardhurave që shqiptarët po i shpenzojnë për shëndetësinë po rritet me ritme mjaft të larta. Sipas të dhënave, nga Qendra Shqiptare për Tregti me Jashtë, (ACIT), gjatë vitit të kaluar Shqipëria importoi më shumë se 11 miliardë lekë ilaçe. Krahasuar me vitin e kaluar, kjo shifër është 22 për qind më e lartë...
NE FAQEN 25

Kronikë

Vjelja e kanabisit, fshati hap "festivalin" e kallashëve
Krisma në Lazarat. Policia: Nuk u qëllua asnjë helikopter
NE FAQEN 22

Ziza, i sëmurë mendor, por jo në momentin e krimit
Dibër, burg i përjetshëm për vrasësin e 10-vjeçarit
NE FAQEN 11

MOTI

Meteorologët: Fundjava me shi, lamtumirë plazh!
NE FAQEN 21

Futboll

Trajneri tregon si u kontaktua nga zikaltërit që në mars
Prezantohet Murinjo: Interi është një skuadër "speciale"
NE FAQEN 31

INTERVISTA

Hamit Karzai, Presidenti i Afganistanit, kritikohet ashpër se nuk ka luftuar me forcën e duhur korrupsionin në Afganistan. Në një intervistë të fundit, njeriu i amerikanëve rrëfen për lidhjet e koalicionit me zotërit e luftës, pështpërimat mbi influencën e familjes së tij dhe pranon se ndonjëherë marrëveshjet e pista janë të domosdoshme...

NE FAQEN 20

Shqip
NDRYSHE

Cilat janë teknikat e përdorura sot? Çfarë fshihet mbrapa tyre? A janë të efektshme?

Si ruhen të fshehtat në kohën tonë

Kriptografia kuantike, sekreti që ruan sekretin

Shkenca e fshehjes, kamuflimit apo ruajtjes sekret të informacioneve të rëndësishme ka shoqëruar njerëzimin pothuajse në të gjitha etapat e zhvillimit të tij. Që në lashtësi është mundur të konceptohen teknika të sofistikuara për të mbajtur sekret informacionet e rëndësishme. Kjo ka qenë shpeshherë fryt i imagjinatës së jashtëzakonshme të mendjeve më të ndritura. Edhe atëherë, informacioni përbënte një nga pikat kyçe për t'u mbrojtur e ruajtur me fanatizëm, duke qenë një nga elementet kryesore të strategjive, si luftarake ashtu edhe civile. Nevoja e epërsisë mbi kundërshtarin, e mbështetur në shkëmbimin e mesazheve sekrete, ka përcaktuar shpesh jo vetëm fatin e luftërave të mëdha, por edhe zhvillimet ekonomike dhe teknologjike. Kjo temë kaq enigmatike, por aq dhe reale, ka qenë dhe mbetet një nga subjektet më të preferuara të kinematografisë apo të letërsisë botërore. Në një botë ku të tërë bien padyshim dakord me postulatin "Kush zotëron informacionin, ka edhe fuqinë", shkëmbimet sekrete të informacioneve përbëjnë një nga subjektet kryesore të kërkimeve shkencore. Po cilat janë teknikat e përdorura sot në këtë fushë? Çfarë fshihet mbrapa tyre? Cila është siguria që këto teknika ofrojnë? Siç e theksuam edhe më sipër, jo vetëm sot, por që në kohët më të lashta informacioni përbënte një nga objektet më të rëndësishëm strategjikë për t'u mbrojtur. Ky problem u bë aq më shumë real me zhvillimin dhe përhapjen e teknologjive të informacionit dhe mbrojtja e këtij të fundit është bërë akoma dhe më e nevojshme...

NE FAQET 14-15

FOTO FAKT

Një çift skocez ka zgjedhur një vend shumë të veçantë për të thënë "po"- në e jetës. Pavarësisht nga mjegulla e shiu, dy të rinj nga Glasgow kanë vendosur të lidhin martesë në majën më të lartë të Urës së Portit në Sidnej të Australisë. Kjo urë është një vend shumë i veçantë, por njëherazi edhe i rrezikshëm

Cilësitë dhe defektet e krijesës që do të donit të kishit përkrah

A ekziston gruaja perfekte?

Përmasat perfekte të një gruaje nuk janë 90-60-90. Nëse e gjithë jeta do të kalohet nën një çati, atëherë është mirë të ulesh në tavolinë me një letër e stilolaps në dorë dhe të përdorësh një metër profesionistësh. Këtë të fundit ua ofron doktor George W. Crane, psikolog në Universitetin Northwestern dhe krijuesi i testit "gruaja perfekte" (pas pak kohësh do të publikohet edhe testi i burrave perfektë), në të cilin fiton më shumë pikë gruaja që nuk ankohet kurrë, preferon pizhame, në vend të këmishës së natës, nuk e kundërshton kurrë bashkëshortin dhe të dielën e lë të pushojë...

NE FAQEN 19

IVANKA TRUMP

Një vajzë në gjurmët e babait

Është e bukur, ambicioze dhe një biznesmene e zonja Ivanka Trump, vajza 26-vjeçare e manjatit amerikan Donald Trump. Për më tepër, është e re, inteligjente dhe ka arritur të diplomohet shkëlqyeshëm në Universitetin e Pensilvanisë. Për revistën e famshme ekonomike "Forbes", Laureta Ivanka Tramp udhëheq edhe klasifikimin e dhjetë trashëgimtareve më sensuale në botë. Ivanka, e cila aktualisht është zëvendëspresidente e Agjencisë së Pronave të Patundshme, pjesë e shoqërisë së të atit "Trump Organisiation", tregon se nuk i trembet botës së egër të biznesit që dominohet vetëm nga meshkujt. Ajo ka si qëllim të ecë sa më lart. Zyrat e familjes Trump gjenden në katin e 25-të, në kullën "Trump" në bulevardin "Fifth Avenue" në Nju Jork, në oazin e qetësisë. Në të majtë ndodhet një sallë gjigante mbledhjesh plot karrige të bukura lëkure, ndërsa në të djathtë një pikturë e madhe me pamje nga parku i gjelbër i qytetit. Përballë, dy asistente tregojnë se zonjusha Trump nuk ndodhet aty për të dhënë intervistën, pasi ka shkuar në qendër të qytetit...

NE FAQEN 18

Nevoja e epërsisë mbi kundërshtarin, e mbështetur në shkëmbimin e mesazheve sekrete, ka përcaktuar shpesh jo vetëm fatin e luftërave të mëdha, por edhe zhvillimet ekonomike dhe teknologjike. Kjo temë kaq enigmatike, por aq dhe reale, ka qenë dhe mbetet një nga subjektet më të preferuara të kinematografisë apo të letërsisë botërore

Kriptografia kuantike: sekreti që ruan sekretin

IGLI TASHI DHE PROF. SOLANGE GHERNAOUTI - HÉLIE
UNIVERSITETI I LOZANËS

Shkenca e fshehjes, kamuflimit apo ruajtjes sekret të informacionit ka shoqëruar njerëzimin pothuajse në të gjitha etapat e zhvillimit të tij. Që në lashtësi është mundur të konceptohen teknika të sofistikuara për të mbajtur sekret informacionet e rëndësishme. Kjo ka qenë shpeshherë fryt i imagjinatës së jashtëzakonshme të mendjeve më të ndritura. Edhe atëherë, informacioni përbënte një nga pikat kyçe për t'u mbrojtur e ruajtur me fanatizëm, duke qenë një nga elementet kryesore të strategjive, si luftarake ashtu edhe civile. Nevoja e epërsisë mbi kundërshtarin, e mbështetur në shkëmbimin e mesazheve sekrete, ka përcaktuar shpesh jo vetëm fatin e luftërave të mëdha, por edhe zhvillimet ekonomike dhe teknologjike. Kjo temë kaq enigmatike, por aq dhe reale, ka qenë dhe mbetet një nga subjektet më të preferuara të kinematografisë apo të letërsisë botërore. Në një botë ku të tërë bien padyshim dakord me postulatin "Kush zotëron informacionin, ka edhe fuqinë", shkëmbimet sekrete të informacioneve përbëjnë një nga subjektet kryesore të kërkimeve shkencore. Po cilat janë teknikat e përdorura sot në këtë fushë? Çfarë fshihet mbrapa tyre? Cila është siguria që këto teknika ofrojnë?

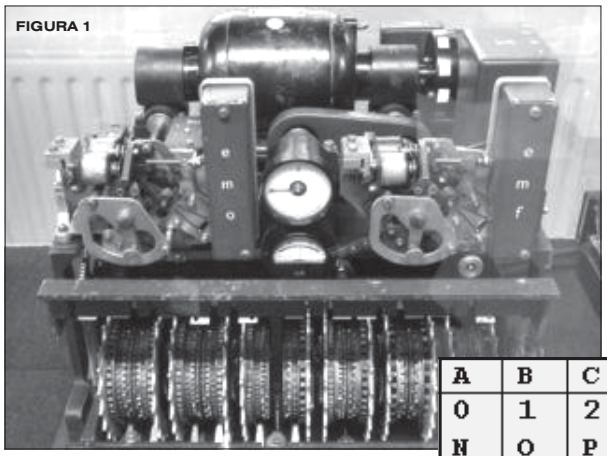


FIGURA 1 - Aparat kriptografik i përdorur nga gjermanët gjatë Luftës së Dytë Botërore

Mjedisi në të cilin qarkullon informacioni

Siç e theksuam edhe më sipër, jo vetëm sot, por që në kohët më të lashta informacioni përbënte një nga objektet më të rëndësishëm strategjikë për t'u mbrojtur. Ky problem u bë aq më shumë real me zhvillimin dhe përhapjen e teknologjive të informacionit dhe mbrojtja e këtij të fundit është bërë akoma dhe më e nevojshme. Kjo, për dy arsye:

1. Së pari, sepse çdo aktivitet, qoftë ai ushtarak, ekonomik, industrial apo i çfarëdo lloji tjetër, mbështetet në shkëmbimin e informacionit, duke i dhënë informacionit një rol primar në funksionimin e shoqërisë së sotme.

2. Së dyti, pasi ky informacion do të transmetohet i dixhitalizuar (në formën numerike, 0 dhe 1), nëpër kanale të cilat nuk mund të jenë subjekt i një kontrolli total dhe me një itinerar të panjohur për dërguesin. A i keni bërë ndonjëherë pyetjen vetes se nga kalon e-mail-i juaj i adresuar një mikut tuaj? Nuk është çudi që ky e-mail të ketë bërë një xhiro nga Japonia, për të kaluar më pas nga Gjermania, për t'u zhytur njëherë nën Atlantik e për t'u ndalur e pushuar pak në Amerikë, duke rinisur udhëtimin e tij deri te destinacioni... ndoshta komshiu i katit të dytë. Nejse, për të mos u zgjatur dhe për të mos u thelluar në funksionimin e asaj që sot rëndom quhet internet, deshëm vetëm t'ju përcillnim karakterin e rastësishëm (random) të qarkullimit të informacioneve.

Duke pasur parasysh rëndësinë e informacionit, por edhe faktin që si pasojë e një farë komoditeti në dërgimin elektronik të tij lindin edhe faktorët kryesorë të cenueshmërisë së tij. Për rrjedhojë, teknika të sofistikuara filluan të përdoreshin gjithnjë e më shumë, sidomos me përdorimin e gjithanshëm të ordinatorëve. Këto u quajtën teknikat e kriptografisë, ose e thënë ndryshe, të fshehjes së informacionit. Informacioni kishte ndryshuar tashmë suport (teksti nuk shkruhej më nëpër letra dhe nuk mësohej përmendësh) dhe në një epokë ku shpejtësia bëhej gjithnjë e më shumë faktor suksesi, nuk do të kishim më kohë të prisnim ardhjen e korrierit, sepse gjithçka do të vendosej në çdo qindtat e sekondës. Tek e fundit, ndoshta do të ishte thjesht e pamundur mbërritja e korrierit në ndonjë fund oqeani, apo edhe në lartësira të pakapshme nga fiziku njerëzor.

Por sikur të mos mjaftonte kjo dhe nga dëshira për të qenë gjithmonë e më të shpejtë: pa u mësuar mirë me një teknologji, sa hap e mbyll sytë një tjetër zë vendin e saj. Natyrisht më e sofistikuar, më performante... por po aq dhe e panjohur.

Shkenca e kriptografisë

Arti i fshehjes moderne të informacionit përmban 3 elemente kryesore:

1. Informacionin vetë
2. Algoritmin matematik që do të përdoret për procesin e transformimit të informacionit
3. Çelësin kriptografik, i cili do të bëjë që informacioni i lexueshëm të shndërrohet në një tekst të pakuptimtë dhe të palexueshëm

Për të shpjeguar këtë koncept le të marrim një shembull të thjeshtë, duke pasur parasysh që këto teknika të thjeshta janë përdorur që në antikitet, duke ardhur e duke u sofistikuar gjithnjë e më shumë me kalimin e kohës. Megjithatë, principi ngelet i njëjtë.

Le të themi që kemi fjalën tepër sekrete GAZETASHQIP për të transmetuar në një kanal ndoshta të përgjuar.

1. Informacioni vetë = GAZETASHQIP
2. Algoritmi = Çdo germë i korrespondon një numër, si p.sh. në tabelën e mëposhtme:
3. Çelësi = 5 që do të thotë që numrat e algoritmit do të zhvendosen me pesë dhe tabloja algoritmike do të shndërrohet si vijon:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Dërguesi do të fshehë informacionin e rëndësishëm, duke përdorur çelësin pra:

A	B	C	D	E	F	G	H	I	J	K	L	M
5	6	7	8	9	10	11	12	13	14	15	16	17
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25	0	1	2	3	4

Sipas çelësit G=11 dhe sipas algoritmit 11=L
Sipas çelësit A=5 dhe sipas algoritmit 11=F
Sipas çelësit Z=4 dhe sipas algoritmit 4=E
Sipas çelësit E=9 dhe sipas algoritmit 9=J
Sipas çelësit T=24 dhe sipas algoritmit 24=Y
Sipas çelësit A=5 dhe sipas algoritmit 11=F
Sipas çelësit S=23 dhe sipas algoritmit 23=X
Sipas çelësit H=12 dhe sipas algoritmit 12=M
Sipas çelësit Q=21 dhe sipas algoritmit 21=V
Sipas çelësit I=13 dhe sipas algoritmit 13=N
Sipas çelësit P=20 dhe sipas algoritmit 20=U

Pra, mesazhi sekret GAZETASHQIP u shndërrua në LFEJYFXMVNU.

Për të bërë të kundërtën, pra për të deshifruar mesazhin e koduar, tashmë mjafton të njohësh logjikën e shndërrimit dhe sigurisht çelësin. Natyrisht që me kalimin e kohës dhe me perfeksionimin e teknikave, konceptet e algoritmeve dhe të çelësave u bënë gjithnjë e më të komplikuar. Por procedura mbeti e njëjtë: një shndërrim logjik i përforcuar nga një çelës sekret.

Kriptografia në ditët e sotme

Shkëmbimet elektronike, si dhe perfeksionimi i teknikave bëri që algoritme shumë më të ndërlikuara të viheshin në përdorim dhe çelësa po aq të ndërlikuar të përdoreshin për fshehjen e kuptimit të informacionit. Në thelb, e gjitha kjo kishte të bënte me përllogaritje matematike tepër komplekse. Duke pasur parasysh nevojën e një komunikimi elektronik standard, algoritmet e përdorura për të kriptuar informacionin, u bënë publike dhe të njohura për të gjithë. Nuk kishte si të ndodhte ndryshe, pasi automatizmi i procedurave kërkonte një kompatibilitet të plotë ndërmjet kompjuterëve apo çfarëdo lloji tjetër burimi komunikimi.

Në qoftë se do të konsiderojmë aftësitë e përgjuesit tashmë dhe ato do të evoluojnë me të njëjtin ritëm si të dërguesve. Aftësia e tij përllogaritëse u rrit, nga lapsi e letra, kaluam te makina llogaritëse dhe më pas te kompjuteri, procesori i të cilit është i aftë të bëjë disa qindra mijëra llogaritje e kombinacione në sekondë.

Në këtë situatë, i vetmi element sigurie për transmetimet sekrete mbeti çelësi që do të thotë se zbulimi i çelësit (algoritmi apo logjika e përdorur mbeten të njohura), do të lejonte dhe deshifrimin e informacionit. Teknikat e deshifrimit (cryptanalysis) të ndihmuara dhe nga ngritja e aftësisë së llogaritjes, bëri që metodat e kriptimit të bëheshin gjithmonë e më të cenueshme. Kjo, për arsyen se çelësi, tashmë elementi kryesor, ose do të transmetohej fizikisht, ose elektronikisht, duke mbartur me vete rrezikun e zbulimit të tij. Transmetimi fizik ka si rrezik kryesor vjedhjen apo zbulimin e tij, kurse ai elektronik, interceptimin e tij gjatë transmetimit. Është fakt që sot çelësat kriptografikë transmetohen apo magazinohen në rrjet për të qenë të përdorshëm sa më lehtë nga të interesuarit. Është fakt që teknika shumë të thjeshta dhe madje të pakushtueshme ekzistojnë për përgjimet elektronike. Sa për ilustrim, mjetet që munden të përgjojnë trafikun, rrjetin gjenden në shitje pothuajse të lirë me një kosto prej rreth 50 •.

Pra, elementi dhe shqetësimi kryesor i organizmave që dëshirojnë të sigurojnë komunikimin sekret është siguria fizike e suporteve të transmetimit. Një rrjet përbën miliona kilometra përçues (kabllo, fibra optike etj.) gjë që bën të pamundur sigurimin e tyre të plotë nga ana fizike. Ana tjetër e medaljes është kriptimi i çelësit vetë dhe dërgimi tij nëpërmjet kanaleve të konsideruara si të sigurta. Këtu jemi në një situatë, ku mundohemi të sigurojmë elementin e sigurisë me të njëjtën procedurë të cenueshme. Është fakt që fuqia llogaritëse e ordinatorëve është rritur në mënyrë eksponenciale. Kjo do të thotë që përgjuesi do të ketë mundësi të përdorë më shumë kombinacione në më pak kohë, për të arritur në rezultatin e dëshiruar... zbulimin e çelësit. Nga viti në vit fuqia e procesorëve, pra ajo e përllogaritjes, shumëzohet me dhjetë. Këta kompjuterë do të përdoren jo vetëm nga dërguesit, por edhe nga përgjuesit. Dalja në treg e kompjuterëve kuantikë (që përdorin elementet e dritës për përçimin e informacioneve) do të bëjë që fuqia llogaritëse e tyre të shumëzohet me 100, 1000 e akoma më shumë. Pra, në qoftë se për të zbuluar një çelës dikur, dikujt do t'i ishin dashur 3 muaj kohë llogaritje, tashmë disa minuta do të mjaftojnë për të arritur në rezultatin e duhur.

Kriptografia kuantike

Siç e theksuam edhe më sipër, transmetimi i sigurt i çelësit mbetet thembra e Akilit në transmetimet konfidenciale të informacioneve të rëndësishme. Është fakt, që sa më shumë vlerë të ketë informacioni, aq më shumë i motivuar do të jetë përgjuesi në zbulimin e tij. Në një atmosferë të mbarsur nga akte terroriste, nga spiunazhi industrial etj., teknikat tradicionale të kriptografisë nuk janë më të mjaftueshme.

I motivuar nga nevoja për transmetime të sigurta dhe duke vlerësuar cenueshmërinë e kriptografisë klasike, Komuniteti Evropian ka ndërmarrë një projekt të madh, që ka implikuar përfaqësues të shumë shteteve, firmave industriale, institucioneve akademike evropiane. Ky është projekti SECOQC (Development of a Global Network for Secure Communication based on Quantum Cryptography - www.secoqc.net).

Përdorimi i teknologjisë kuantike mbështetet në një investim të qëndrueshëm në kohë, duke anashkaluar kështu efektin e përmirësimit të teknologjisë. Pavarësisht nga teknologjitë e përdorura, vetitë dhe stabiliteti fizik mbetet i njëjtë. Kjo teknologji, pavarësisht inovacionit, nuk e ndryshon strukturën e komunikimit të deritanishëm. Fotonet e dritës mund të përçohen me të njëjtën fibër optike që përdoret edhe sot në komunikimet elektronike

FIGURA 2

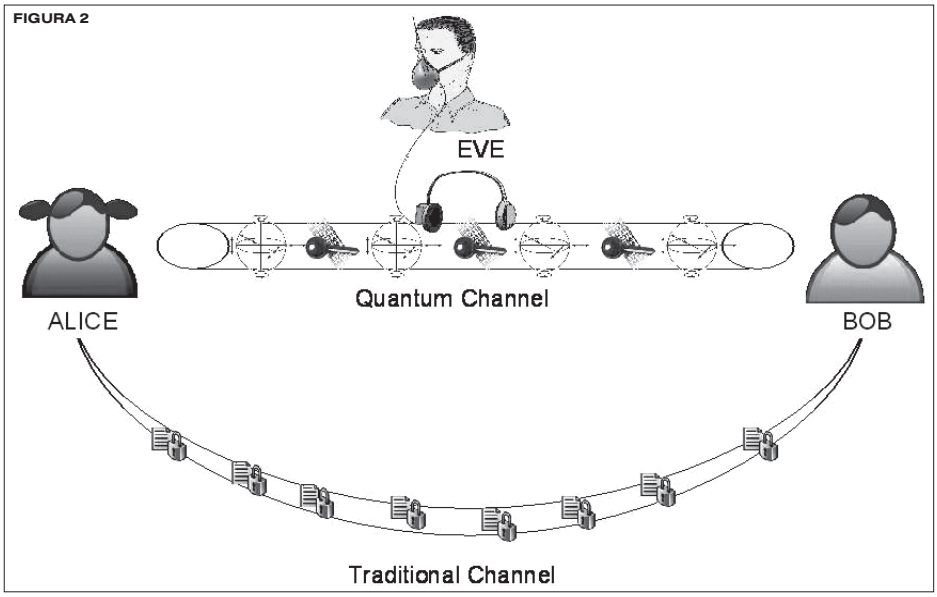


FIGURA 2 - Koncepti i kriptografisë kuantike

Një ndër partnerët e projektit është edhe Universiteti i Lozanës, i përfaqësuar nga ekipi ynë i kërkimit. Ideja është sa e thjeshtë aq dhe e vështirë për t'u vënë në praktikë. Ajo ka të bëjë me përdorimin e fotoneve (grimcave elementare të dritës) si mundësi kriptimi dhe dërgimi i çelësave sekretë kriptografikë. Deri tani çdo informacion i dërguar në mënyrë elektronike kodohet në byte, që do të thotë në një mënyre binare, 0 ose 1. Te kjo thjeshtësi qëndron dhe thelbi i suksesit të informatikës, por edhe i cenueshmërisë së saj. Karakteret alfanumerike (germat, numrat dhe elemente të tjera) shprehen nëpërmjet byte-ve për t'u dërguar në rrjet dhe për t'u interpretuar nga makina që nuk kanë logjikë, pra kompjuterët. Dhe çelësat në fjalë, që janë karaktere alfanumerike, transformohen në seri 0-sh dhe 1-sh për t'u kriptuar e për t'ju transmetuar të interesuarve. Këto çelësa rrezikohen ose nga interceptimi i tyre, ose nga deshifrimi (cryptanalysis) që do të thotë deduksioni i çelësit nga një seri karakteresh të pakuptimtë. Kjo, falë fuqisë së kompjuterëve dhe shpejtësisë llogaritëse të tyre.

Ideja e kriptografisë kuantike është përdorimi i pozicionit të fotoneve të dritës në kodazhin e karaktereve alfanumerike në vend të zerove dhe njëshave. Fotonet e dritës marrin 4 pozicione: horizontale, vertikale, +45° dhe -45°.

Një protokoll komunikimi, që përdor këto veçori të fotoneve, u artikulua nga 2 shkencëtarë kanadezë të quajtur Brassard and Benneth në 1984, nga vjen dhe emri i protokollit BB84.

Siguria që jep ky protokoll, vjen kryesisht nga 2 veçori fizike të fotoneve:

- E para, që fotonet e dritës, ose më saktë pozicionet e tyre nuk mund të kopjohen (interceptohen)
- E dyta, që ata nuk mund as të vëzhgohen gjatë kohës që janë në lëvizje

Në fakt, fotonet e dritës janë grimca shumë të paqëndrueshme, ku ndërhyrja më e vogël bën që ato të dëmtohen (ose të ndryshojnë).

Në rast se dy organizma që duan të komunikojnë në mënyrë konfidenciale bien dakord mbi kuptimin që do t'u japin pozicioneve të fotoneve (p.sh., +45° dhe horizontal = 0 dhe -45° dhe vertikal = 1), do të ishte e pamundur për një përgjues të studionte apo interceptonte këto pozicione gjatë transmetimit.

Në radhë të parë, pasi interceptimi do t'i shkatërronte fotonet dhe kështu çelësi i koduar nuk do të arrinte në destinacion. Pra, si rrjedhojë, nuk do të përdorej për kriptim të informacionit.

Në radhë të dytë, pasi përgjimi apo vëzhgimi i tyre do të ndryshonte komplet pozicionet e duke i dhënë kështu një sinjal pritësit që transmetimi nuk ka qenë i sigurt.

Një tjetër dukuri shumë me rëndësi që ofron shkëmbimi kuantik është dhe fakti i gjenerimit totalisht të rastësishëm (random) të pozicioneve dhe si rrjedhojë të elementeve alfanumerike, që do krijojnë çelësin. Ky është një aspekt shumë i rëndësishëm për arsyen: sa më të rastësishëm të jenë karakteret, aq më e vështirë është të deduktosh kuptimin e tyre. Deduksioni apo kuptimi i mekanizmit apo logjikës së fshehur mbrapa mesazhit apo çelësit të koduar siç thamë edhe me sipër, ishte një nga elementet bazë të deshifrimit.

Kjo mënyrë kodimi e informacioneve sensibël paraqet një përmirësim të paneglizhueshëm të praktikave të fshehjes së informacioneve.

Së pari, rastësishmëria e karaktereve në krahasim me ato informatike të bazuar, gjithsesi, në një logjikë programimi, bën të pamundur deduktimin e logjikës së përdorur.

Transmetimi i çelësave sekretë bëhet në një mënyrë shumë të sigurt dhe bazohet në veti fizike e jo matematike. Kjo do të thotë që siguria e çelësit nuk mund të cenohet nga rritja e aftësisë llogaritëse të mjeteve të përdorura për deshifrim.

Përdorimi i teknologjisë kuantike mbështetet në një investim të qëndrueshëm në kohë, duke anashkaluar kështu efektin e përmirësimit të teknologjisë. Pavarësisht nga teknologjitë e përdorura, vetitë dhe stabiliteti fizik mbetet i njëjtë.

Kjo teknologji, pavarësisht inovacionit, nuk e ndryshon strukturën e komunikimit të deritanishëm. Fotonet e dritës mund të përçohen me të njëjtën fibër optike që përdoret edhe sot në komunikimet elektronike. Mbi këtë bazë të fortë teorike u mbështet edhe projekti ynë, për të formalizuar dhe krijuar infrastrukturën e nevojshme për komunikimin kuantik. Kjo nënkuptonte gjetjen e mekanizmave dhe mjeteve që do të mund të përcillnin në dalje grimca mikroskopike e të paqëndrueshme, si dhe mekanikave e mjeteve që do të mund t'i detektonin në hyrje (receptorë).

Stadi tjetër ishte vendosja e protokollit të komunikimit midis këtyre "kutive të zeza", le t'i quajmë dhe përgjithësimi i idesë për një përdorim sa më të gjerë dhe operativ. Përdorimi i kriptografisë kuantike e ka kaluar tashmë stadin e eksperimentimit, duke u përdorur në disa raste nga organizma të interesuar në komunikimet konfidenciale. I tillë është rasti i disa bankave në Zvicër, apo Austri, apo dhe i disa organizmave shërbimesh inteligjente në Evropë. Një eksperiencë tashmë e konsoliduar është edhe përdorimi i teknologjisë kuantike në procesin e votës nëpërmjet internetit në Kantonin e Gjenevës.

Që prej dy vjetësh, ky kanton ka autorizuar dhe vlerësuar si të sigurt përdorimin e teknologjisë kuantike në votimin në distancë. Kjo teknologji përdoret si për gjenerimin e numrave thellësisht të rastësishëm (random) të identifikimit të votuesve, ashtu dhe në sigurimin e autentifikimin e votuesve, duke bërë që vota të jetë plotësisht e padeshifrueshme dhe si rrjedhojë e pamanipulueshme deri në destinacion.

FIGURA 3

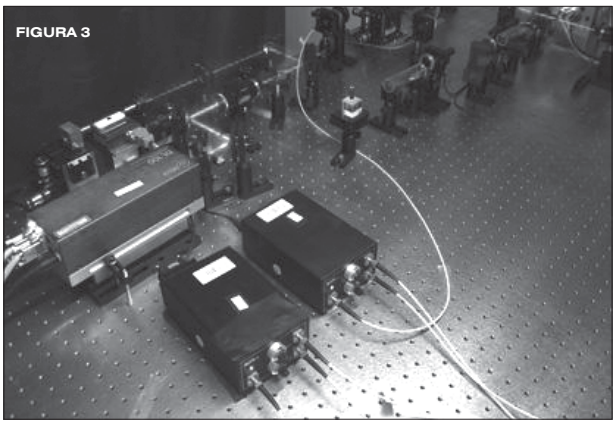


FIGURA 3 - Një demonstrim i funksionimit të kriptografisë kuantike

FIGURA 4 - Procesi i përdorimit të kriptografisë kuantike në votimin elektronik

Sigurisht që si teknologji e re, kriptografia kuantike paraqet për momentin kosto që nuk janë akoma të përballueshme nga të gjithë. Megjithatë, një përdorim masiv i kësaj teknologjie (siç janë dhe premisat që ne kemi vëzhguar e analizuar deri më tani në terren), do të sjellë një ulje drastike të kostove.

Megjithatë, vlen të theksohet fakti që rëndësinë dhe vlerën e informacionit, mund t'ia japë vetëm ai që e mban. Është po i njëjti person që do të bëjë vlerësimin nëse një teknologji si ajo kuantike është e nevojshme për të mbrojtur vlerën që mbart informacioni. Tek e fundit, informacioni është si një foto e vjetër, vetëm ai që e ruan e njeh vlerën e tij .

Elementi dhe shqetësimi kryesor i organizmave që dëshirojnë të sigurojnë komunikimin sekret është siguria fizike e suporteve të transmetimit. Një rrjet përbën miliona kilometra përçues (kabllo, fibra optike etj.) gjë që bën të pamundur sigurimin e tyre të plotë nga ana fizike

FIGURA 4