IT'14
ŽABLJAK

XIX

naučno - stručni skup

INFORMACIONE TEHNOLOGIJE

SADAŠNJOST I BUDUĆNOST

Urednik
Božo Krstajić

IT'14

INFORMACIONE TEHNOLOGIJE

- SADAŠNJOST I BUDUĆNOST -

Urednik
Božo Krstajić

Zbornik radova sa XIX naučno - stručnog skupa
INFORMACIONE TEHNOLOGIJE - sadašnjost i budućnost
održanog na Žabljaku od 24. do 28. februara 2014. godine

Zbornik radova
INFORMACIONE TEHNOLOGIJE - sadašnjost i budućnost 2014

Glavni urednik
Prof.dr Božo Krstajić

Izdavač
Univerzitet Crne Gore
Elektrotehnički fakultet
Džordža Vašingtona bb., Podgorica
www.etf.ucg.ac.me

Tehnička obrada
Aleksandra Radulović
Centar Informacionog Sistema
Univerziteta Crne Gore

Tiraž
150

Podgorica 2014.

Organizator

Elektrotehnički fakultet Univerziteta Crne Gore

Skup su podržali:

* Ministarstvo za informaciono društvo i telekomunikacije
* Pošta Crne Gore
* Agencija za elektronske komunikacije i poštansku djelatnost
* Čikom

Programski odbor

Dr Novak Jauković, Elektrotehnički fakultet, Podgorica
Akademik Dr Ljubiša Stanković, CANU
Dr Zdravko Uskoković, Elektrotehnički fakultet, Podgorica
Dr Vujica Lazović, Ekonomski fakultet, Podgorica
Dr Branko Kovačević, Elektrotehnički fakultet, Beograd
Dr Milorad Božić, Elektrotehnički fakultet, Banja Luka
Dr Miroslav Bojović, Elektrotehnički fakultet, Beograd
Dr Zoran Jovanović, Elektrotehnički fakultet, Beograd
Dr Božidar Krstajić, Elektrotehnički fakultet, I. Sarajevo
Dr Milica Pejanović-Đurišić, Elektrotehnički fakultet, Podgorica
Dr Dejan Popović, Elektrotehnički fakultet, Beograd
Dr Božo Krstajić, Elektrotehnički fakultet, Podgorica
Dr Milovan Radulović, Elektrotehnički fakultet, Podgorica
Dr Budimir Lutovac, Elektrotehnički fakultet, Podgorica
Dr Igor Radusinović, Elektrotehnički fakultet, Podgorica
Dr Igor Đurović, Elektrotehnički fakultet, Podgorica
Dr Miloš Daković, Elektrotehnički fakultet, Podgorica
Dr Milutin Radonjić, Elektrotehnički fakultet, Podgorica
Dr Ramo Šendelj, Fakultet za Informacione Tehnologije, Podgorica
Dr Stevan Šćepanović, Prirodno-matematički fakultet, Podgorica
Dr Sašo Gelev, Elektrotehnički fakultet, Radoviš

Organizacioni odbor

Dr Božo Krstajić, Elektrotehnički fakultet, Podgorica
Dr Milovan Radulović, Elektrotehnički fakultet, Podgorica
Dr Ana Jovanović, Elektrotehnički fakultet, Podgorica
Dr Saša Mujović, Elektrotehnički fakultet, Podgorica
MSc Žarko Zečević, Elektrotehnički fakultet, Podgorica
Vladan Tabaš, dipl.ing., Čikom

Sekretarijat

Aleksandra Radulović, CIS Univerzitet Crne Gore

P R E D G O V O R

Poštovani učesnici i čitaoci,

Pred vama je zbornik radova koji su prezentovani na XIX Naučno-stručnom skupu "INFORMACIONE TEHNOLOGIJE – sadašnjost i budućnost" (IT'14) koji je uspješno održan od 24. do 28. februara 2014. godine na Žabljaku. U cilju sveobuhvatnog i multidisciplinarnog sagledavanja aktuelnosti u oblasti informaciono-komunikacionih tehnologija u Crnoj Gori i svijetu, Programski odbor je izvršio selekciju kvalitetnih radova čiji su rezultati bili prezentovani učesnicima Skupa, dostupni svim korisnicima Interneta preko web sajta www.it.ac.me I konačno vama putem ovog zbornika. Konstantno povećanje broja prijavljenih i prezentovanih radova, sve širi krug eminetnih naučnika uključenih u proces recenzije i izbor najboljih radova koji će se štampati u časopisu Elektrotehničkog fakulteta Univerziteta Crne Gore u Podgorici ("ETF Journal of Electrical Engineering") su jasna potvrda uvećanju kredibiliteta i kvaliteta konferencije.

U okviru Skupa je održana radionica „Razvoj mobilnih aplikacija", okrugli sto "IXP4ME – potreba i dileme" i prezentovani projekti: "Fostering innovation based research for e-Montenegro – Fore-Mont", "ECDL za digitalnu Crnu Goru", "Wireless Montenegro" i „Open Govrenment Data (OD) inicijative u Crnoj Gori".

U ime organizatora skupa se zahvaljujem svima koji su na bilo koji način učestovali u radu ovogodišnje konferencije i najavljujem posebno osmišljen i bogat program za naredni-jubilej XX IT.

Sve detalje o ovom, prošlim i narednom skupu možete naći na poznatoj adresi www.it.ac.me.

Prof. dr Božo Krstajić

SADRŽAJ

IZBOR OPTIMALNE TEHNIKE ZA ENKRIPCIJU I DEKRIPCIJU PODATAKA
SELECTION OF OPTIMAL TECHNIQUES FOR ENCRYPTION AND DESCRYPTION OF DATA

Ilija Apostolov, Risto Hristov, *Evropski Univerzitet Republika Makedonija –Skopje*
Sašo Gelev, *Elektrotehnički fakultet - Radoviš*

Sadržaj: *Enkripcija pretstavlja proces konvertiranja jednostavne tekst poruke u šifrirani tekst koij moze biti dekodiran u originalnom tekstu. Enkripcija i dekripcija se sprovodi putem algoritma kojeg možemo implementovati u programskom jeziku. Razgledaćemo potrebe za zaštitu podataka, kao i nacine enkripcije i njihove algoritme. Daćemo predlog za enkripciju e-mail poruke. Zatim ćemo pričati o potrebama za enkripciju i pretstavićemo način podsticaja za korišćenje enkripcijskih tehnika. Veliki broj softverskih rešenja uspešno se spravljaju sa zaštitom prilikom prenosa podataka, e-mail enkripcije i enkripcije celih diskova.*

Abstract: - *Encryption is the process of converting simple text message in the encoded text that can be decoded back to the original message. The method of encryption and decryption of data is implemented by an algorithm that can be implemented in a programming language. We will review the needs for data protection and encryption types and their algorithms. We will also make suggestions for encrypting e- mail messages. Then we will talk about the need for encryption and we will demonstrate the way to encourage the use of encryption techniques. Many software solutions are successfully deal with the protection of data transmission, e- mail encryption and decryption of entire hard disks.*

1. UVOD

Pre pedeset godina algoritme za enkripciju su koristili samo najbolji računari u svetu. Danas imamo potrebu da obezbedimo podatke u našim računarima. Podaci se moraju obezbediti od krađe ili gubljenje. Troškovi povezani sa gubitkom podataka su nepredvidivi, a osim vremena i novca, može da uključi i gubitak pouzdanosti kompanije i iznošenje tajne u javnost. Potreba za sigurnijom zaštitom je sve veća i zato IT lica troše sve više vremena i resurse na ovoj problematici. Programeri za enkripciju obezbeđuju rešenja koja nude sveobuhvatnu skalabilnu zaštitu koja ne dozvoljava otvoreni pristup do sve tačke kompanije, organizacije ili do podataka koji su spodeljeni na mreži [1].
Kriptografija je nauka koja proučava bezbedno zapisivanje. U svim novim tehnologijama i tehnikama stari način kriptiranja i dekriptiranja podataka zamenjen je novim sofisticiranijim načinom koji velikom lakoćom bezbedno čuva naše podatke[2]. U suštini, kriptografski algoritam predstavlja sklop matematičkih funkcija koje koristimo za enkripciju i dekripciju podataka [3]

A. Kodiranje naspram dekodiranja

Slika 1. Proces enkripcije i dekripcije

Kodiranje predstavlja interpretacija reći ili fraza u druge reći i fraza. Ova dva procesa omogućavaju šifrovano prevođenje pisama ili simbola pojedinačno. U suštini, enkripcija kao termin obuhvata enkripciju i šifrovanje. Naspram toga, dekripcija obuhvata dekodiranje i dešifrovanje [3].

B. Principi enkripcije

Kriptografija može biti i jaka i slaba. Rezultat jake kriptografije je šifrovan tekst kojeg je teško dešifrovati ako nemaš specijalnu alatku za dekodiranje ili ako ne poznaješ algoritam koji je korišten za šifrovanje poruke [4]. Na internetu možemo naći veliki broj besplatnih softvera za enkripciju, ali za bolja softverska rešenja kompanije naplačuju za uloženi rad u izradi ovih moćnih programa koji se oslanjaju na matematičke i ostale korisne algoritme koji su pričina za njihovo odlično funkcionisanje. Danas je većina ovih algoritama implementirana u večinu popularnih programskih jezika.
Prve primene kriptografije nalazimo još u vreme Julije Cezara. On je svoj algoritam definisao na taj način što pomera alfabetu za tri pozicije u desno i odbacuje zadnja tri slova, u ovom slučaju X,Y, i Z. Danas se ovaj način ne računa bezbednim, ali u to vreme je dobro funkcionisao. Onaj koji prima poruku da bi je pročitao mora pomerite slova za tri mesta unazad da bi je pročitao [5].

Primer : A B C D E…
↓ ↓ ↓ ↓ ↓
D E F G H…

Radi obezbeđivanje poverljivosti kriptografija koristi sledeće principe:

Autentifikacija: U ovom procesue primač enkriptirane poruke mora utvrditi poteklo poruke.

Integritet: Primaoc poruke mora biti sposoban da vidi dali je poruka promenjena za vreme njenog putuvanja. Napadać ne može zamenite original lažnom porukom.

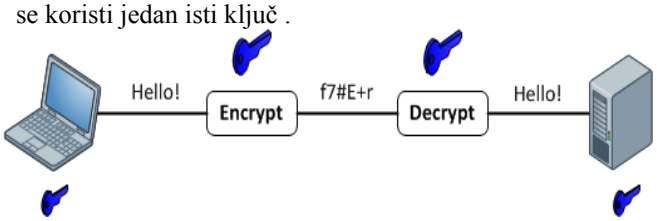
Nepoštovanje: Ni u jednom slučaju pošiljalac ne sme da negira da je poruka od njega poslata.

Poverljivost: Poruka mora biti tako enkriptovana da je nitko drugi sem nas ne može pročitati [5].

2. VIDOVI ENKRIPTIRANJA PODATAKA

Simetrična enkripcija

Simetrična enkripcija ili poznata i kao spodeli ključ. U simetričnoj enkripciji za kriptiranje i dekriptiranje podataka se koristi jedan isti ključ .



Slika 2. Primer za simetričan način enkripcije i dekripcije podataka

Simetrična enkripcija sadrži brye algoritme jer imaju relativno malu kompleksnost koja dozvoljava lako prilagođavanje hardveru [6]. Ipak, ovi algoritmi traže da svi glavni računari koji se koriste u ovom procesu, prethodno budu konfigurisani tajnim ključem. Tajni ključevi se koriste u procesu enkripcije da bi izbegli neovlaščeni pristup napadača, koji kasnije može sebe da predstavi kao pošaljioca poruke. Zatim se dekripcija vrši kod primaoca poruke, koji dekriptira poruku kopijom ključa pošaljioca [7].

1.1 DES (Data Encryption Standard)

Krajem šesdesetih godina dvadesetog veka razvojem finansiskih transakcija, kriptografija je bla sve više interesantna korisnicima. Javila se potreba šifrovanja kojeg bi koristili ljudi širom sveta, tj javila se potreba poverljivosti koja bi bila uspostavljena uvođenjem standarda u kriptografiji [8].

1973 godine Američki institut za standardizaciju i tehnologiju (NIST) imao je za cilj da kreira program za zaštitu računarskih i komunikacijskih podataka. Raspisali su tender za razvoj standardnog sistema kriptografije. Kompanija IBM je ponudila algoritam. Ovaj se algoritam zasnovao na šifrovanje Horsta Feistela. Predloženi algoritam je nakon nekoliko modifikacija bio prihvačen kao standar 1976 godine pod imenom Data Encryption Standard (DES). Ovaj standar enkriptira i dekriptira blokove od 64 bita i koristi ključ veličine 56 bita [9].

Kasnije kao zamena za DES standar ponuđen je standard 3DES (Triple Data Encryption Standard) koji je bio odobren od FIPS (Federal Information Processing Standards Publications) koji obuhvata kriptografske zahteve za kriptografse module. Sve više vladinih organizacija u Americi i širom sveta prihvataju 3DES standard kao osnovu razumne strategije koja preuzima zaštitne mere povezane sa rizikom od napadača i neželjenih efekata[10][9].

1.2 AES (Advanced encryption standard)

Ovaj standard za enkripciju podataka odobren je od FIPS (Federal Information Processing Standards Publications). [10] Enkriptira i dekriptira 128 bitne blokove i koristi ključeve veličine 128, 192 ili 256 bita.

Kao i većinom algoritama simetrične enkripcije, i AES koristi iste korake u procesu enkripcije i dekripcije. Ovaj algoritam radi na bajtima i to ga čini lakšim za implementaciju i objašnjavanje. Za vreme šifrovanja, ključ se proširuje u individualne podključeve, koji se koriste za svuku operaciju zasebno. Ovaj process nazivamo ekspanzijom ključeva [11].

Operacije se izvodi više puta od strane standarda AES koji radi sa fiksnim brojem bajti [12].

Ove operacije mogu biti probijene upotrebom nekoliko funkcija koji će biti deo našeg budućeg istraživanja:

- ADD ROUND KEY
- BYTE SUB
- SHIFT ROW
- MIX COLUMN

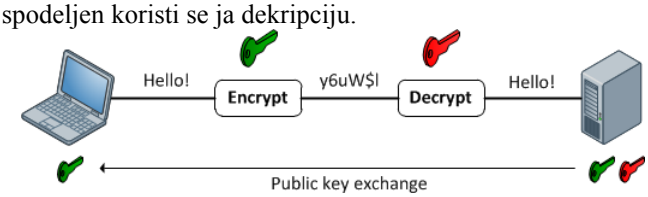
1.3 Drugi poznati simetrični algoritmi

- Triple DES (ECB, CBC), DESX, GDES, RDES – Ključ dužine 168 bita
- (Rivest) RC2, RC4, RC5, RC6 – Promenljiva dužina ključeva do 128 bita
- IDEA – Osnovni algoritam za PGP – ključ dužine 128 bita
- Blowfish – – Promenljiva dužina ključeva do 448 bita
- Twofish – Šifrira 128-bitne blokove otvorenog teksta sa dužinom ključeva do 256 bita

Asimetrična enkripcija

Asimetrična enkripcija, poznata još i kao kriptografija javnim ključevima. Razlikuje so od simetrične enkripcije time što se koriste dva ključa, jedan u vreme enkripcije, a drugi za vreme dekripcije. Najčesće korišteni algoritam asimetrične enkripcije je RSA algoritam.

U poređenju sa simetričnom enkripcijom, asimetrična enkripcija nameće veće opterećenje u vreme računanja, Najavljuje se da će bidi usavršen. Ali, glavni zadatak ove enkripcije je da uspostavi betbedan medij. Ovo se postiže razmenom javnih ključeva koi se mogu koristiti samo za enkripciju podataka. Dodatni privatni ključ, koji nikada nije spodeljen koristi se ja dekripciju.



Slika3. Primer asimetrične enkripcije i dekripcije podataka

Najprije, krajnje tačke razmenuju javne ključeve, što omogučava spor ali siguran protok. Zatim, pošaljilac i primaoc odlučuju da razmene ključeve simetrične enkripcije, čime so omogučava brz protok podataka kroz ove kanale [12].

Algoritmi asimetrične enkripcije

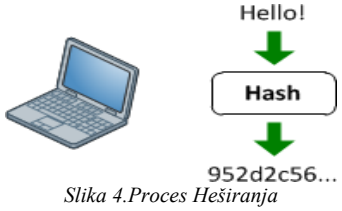
1.1 RSA algoritam

Ovaj algoritam je zasnivam na težini razlaganja velikih brojeva koji imaju samo 2 prosta broja. Javni ključ je dostupan svakome i ovim ključem možemo kriptirati podatke ali ih ne možemo dekriptirati. Ove podatke može dekriptovati samo onaj koji poseduje privatni ključ. Teorijski je moguče, ali u praksi je mnogo teško generirati privatni ključ na bazi znanja javnog ključa. Sve ovo pravi da RSA algoritam bude mnogo popularan izbor za enkripciju podataka [13].

Hashing

Hashing predstavlja forma kriptografske bezbednosti koja se razlikuje od enkripcije. Enkripcija u suštini predstavlja

process u dva koraka, enkripcija i dekripcija. Hashing kondenzuje poruku fiksne dužine. Dva najupotrebljavana algoritma za Hashing su MD5 i SHA-1. Hashing se upotrebljava da bi promenili podatke u bezbednijem obliku, a originalna poruke se ne može vratite nazad.



Slika 4.Proces Heširanja

Kada koristimi haš za autentifikaciju za bezbedno komuniciranje, on pretstavlja rezultat originalne poruke plus tajni ključ. Haš algoritam se koristi i bez tajnog ključa za pruveru grešaka [14].

3. PREGLED PROGRAMA ZA ENKRIPCIJU E-MAIL PORUKA

Potreba upotrebe softvera za enkripciju e-mail poruka javlja se bez obzira dali smo uključeni u osetljive finansiske transakcije, dali imamo privatnu bižnis potrebu ili smo deo neke kompanije koja radi sa poverljivim podatcima. Cilj je da se uspostavi poverljiva komunikacija sa drugom osobom.

Slika 5.Pregled najboljih enkripcijskih programa za enkripciju e-mail poruka

Ovi softveri omogućavaju besprekornu zaštitu nama i našim podatcima. Iako su unešeni algoritmi teški za shvatanje, najvažnije je to što imamo zaštićene poruke.[3]

Svi programi imaju slične koncepte održavanja privatnosti poruka, ali nisu svi isto efikasni. Programi sa jakom enkripcijom omogućavaju da enkriptujemo e-mail poruke velikom lakoćom. Deo najboljih programa u maju 2013 godine na osnovu rangiranja web sajta www.toptenreviews.com su: Voltage SecureMail, Entrust, Comodo, Symantec i dr . Na slici 5 prikazana su 10 najbolja softverska rešenja koji nude zaštitu e-mail poruka. Obuhvaćeni su delovi: Zaštita podataka, Mogućnosti, Klijenti koji mogu da se povežu (pr. Microsoft Outlook) kao i podržane platforme. Nakon izvršenih ispitivanja kao najsigurniji se pokazao Voltage koji naplačuje svoje usluge. Ovaj softver koristi svoj algoritam (IBE Algorithm). Ali, iako je spored nih najsigurniji, ipak nije i najisplatljiviji. Kao predlog za enkripciju nudimo softver Comodo. Comodo je besplatan i daje jaku enkripciju. Comodo pruža enkripciju putem digitalnih sertifikata i koristi se kao dodatak u nekim klijentima koji se sinhronizuju sa našim e-mailom (Pr. Microsoft Outlook). Uradili smo prakticno ispitavanje programom Comodo i pokazalo se da je lak za upotrebu.

4. POTREBA ZA ENKRIPCIJU PODATAKA U R.MAKEDONIJI

Veliki je broj softverskih alata koji se nude za enkripciju na internetu. Deo njih je besplatan, a deo nakon isteka probnog perioda od 30 dana naplačuju svoje usluge. Sva ova softverska rešenja kreirana su implementacijom nekih od algoritama o kojima smo pisali. U principu skoro svi programi koriste slične algoritme. Ipak je potrebno da se sporede. Ova upoređenje od aspekta preopterećenja računarske konfiguracije, efikasnog rada i potrebnih finansijskih sredstava za nabavku softvera pomoći će nam u odlučivanje koji programa i koja tehnika za enkripciju i dekripciju podataka je najoptimalnija.

U R.Makedoniji je neophodno istraživanje kolika je potreba od upotrebe kriptiračkih programa, što računamo kao naš sledeći izazov. Takođe se mora ponuditi i rešenje za korisnike koji nisu upućeni u ovu problematiku. Kao sledeći problem nameće se finansijska mogućnost onih koji imaju potrebu da kriptiraju bilo kakav podatak.

5. PODSTICAJ ZA KORIŠĆENJE ENKRIPTIRAČKIH TEHNIKA ZA BEZBENOST PODATAKA

Sve nas interesuje koliko korporacijskih podataka se šalje bezbedno i kako se šalju. Često smo svedoci da se u kancalarijama zaboravljaju otvorene e-mail poruke koje mogu da sadrže senzitivne podatke. Odavde dolazi i potreba o upotrebi najoptimalnijih tehnika i zaštita podataka [15].

Urađeno je istraživanje u opštini Negotino i Agenciji za ruralni razvoj R. Makedonije i dobivena je slika koliko su sigurni korporacijski podati u ovim institucijama i koliko se koriste tehnike enkripcije i dekripcije podataka.

Opština Negotino oupšte ne koristi softver za enkripciju i dekripciju podataka, e-mail poruka ili softver za enkripciju celog diskovnog prostora.

U Agenciji za ruralni razvoj koriste napredna softverska rešenja za enkripciju podataka. Koriste softver „PGP“ za enkripciju prilikom razmene podataka, ali koriste i druga softverska rešenja za enkripciju diska i podataka „TrueCrypt“ i „Boxcryptor“. Program Boxcryptor se upotrebljava za mauntiranje disk particije bilo kojeg računara u instituciji, i kasnije se pravi backup (rezervna kopija) na specijalnom “Arkeia backup appliance“.

Na osnovu našeg istraživanja dali smo predlog za izbor optimalne tehnike za enkripciju i dekripciju podataka. Za enkripciju e-mail poruka u obe institucije smo predložili rešenje Comodo, koje nudi jaku zaštitu, ali smo im pretstavili i program Voltage koji pruža daleko bolju enkripciju e-mail poruka. Naišli smo na pozitivnu reakciju rukovodstva i zapošljenih, i očekujemo da će isto biti sprovedeno i u drugim institucijama i kompanijama. U agenciji ruralnog razvoja trenutno je dobra enkripcijska zaštita, ali u opštini

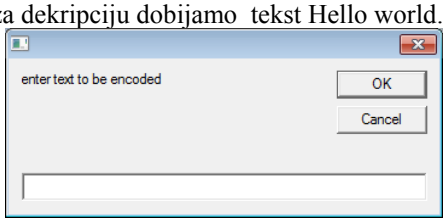
Negotino smo predložili više rešenja za enkripciju particije hard diska ili celog diska. U obe institucije smo predložili jednostavan način tekst enkripcije i dekripcije kojeg nude Windows XP, Vista i Windows 7, što dodatno može uticati na zaštitu tekstualnih poruka ili mnogu važnih elektronskih dokumenata. U suštini to su dva VBScript files koji u sebe sadrže kod, jedan za enkripciju, a drugi za dekripciju.

Slika 6. VBScript filesya tekst enkripciju I dekripciju

Ove fajlove kreiramo nakon unošenja u najobicniji text file i snimamo kao „encode.vbs“. Enkriptiracki kod je:

```
'SIMPLE VB ENCRYPTION PROGRAM'
'Create a dialogue box that asks for the text to encode'
set x = WScript.CreateObject("WScript.Shell")
mySecret = inputbox("enter text to be encoded")
'Reverse the submitted text'
mySecret = StrReverse(mySecret)
'Open up an instance of Notepad to print the results after waiting for 1
second'
x.Run "%windir%\notepad"
wscript.sleep 1000
x.sendkeys encode(mySecret)'this function encodes the text by advancing
each character 3 letters'
function encode(s)
For i = 1 To Len(s)
newtxt = Mid(s, i, 1)
newtxt = Chr(Asc(newtxt)+3)
coded = coded & newtxt
Next
encode = coded
End Function
```

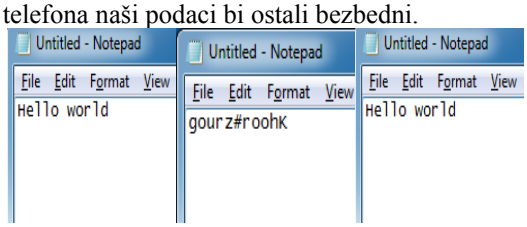
Slično izgleda i program za dekripciju. Primer ako u programu za enkripciju ubacimo tekst Hello world dobijamo kriptiran tekst gourz#roohK. Ako ovaj tekst ubacimo u program za dekripciju dobijamo tekst Hello world.



Slika 7. VBScript jednostavan program za tekst enkripciju

VBScrypt fajlovi su bazirani na RC4 enkriptirackom algoritmu. RC4 se koristi i u WEP, WPA, SSL, BitTorrent, PDF i sl. On je jednostavan za razumevawe i implementaciju. Veliki broj ljudi u R.Makedoniji koji rade sa korporativnim podacima nusu svesni o mogućnosti neželjenih napadača koji za cilj imaju zloupotrebu nekih podataka.

Razgledana je mogućnost funkcioniranja ovih tehnika na više operativnih sistema i platformi, a ne samo na računare, već i za smart telefone, a kao predlog za Android platformu nudimo Secret Space Encrytor. On bezbedno čuva lozinke naših profila na e-mail adresama, kreditnim karticama ili lozinke drugih profila. Takođe, može da enkriptira cele datoteke telefonskih uređaja, tako da u slučaju gubljenja našeg telefona naši podaci bi ostali bezbedni.



Slika 8.Prikaz tekst enkripcija i dekripcija

6. ZAKLJUČAK

U današnje vreme kada su računari i računarske mreže svuda oko nas, zaštita podataka je sve značajnija. Veliki broj ljudi pokušavaju na razne načine da naruše bezbednost računarskih mreža, da bi nekome naštetiili ili imali nekakvu dobit od toga.

Napadači pokušavaju da pročitaju ili da promene sadržaj podataka koja su im dostupna na mreži. Zato je neophodno razviti inteligentne tehnike kako bi računarske mreže i podatci u njima bili bezbedni. Zadovoljavajući rezultati dobiveni upotrebom raznih algoritama za enkripciju su dobra osnova za dalja istraživanja. Tehnike za enkripciju, protokoli autentifikacije i pojava digitalnih potpisa i SSL protokola, omogućavaju siguran način izvođenja bankarskih transakcija i razmena dokumenata velike važnosti.

Danas kada je čitav svet povezan globalnom mrežom, neophodna je kriptografija kako bi imali svoji privatnost.

LITERATURA

[1] Phil Zimmermann, The Basics of Cryptography, An Introduction to Cryptography, Copyright 1990–2000 Network Associates, Inc. and its Affiliated Companies.

[2] Peter Mathys, Introduction to Cryptography, ECEN 1200, Telecommunications 1, Fall 2006.

[3] H.Lee Kwang, Basic Encryption and Decryption, Department of Electrical Engineering & Computer science, KAIST.

[4] Paul Krzyzanowski, Lectures on distributed systems, Cryptographic communication and authentication, 1997-2009 .

[5] Dennis Luciano and Gordon Prichett, Cryptology: From Caesar Ciphers to Public-Key Cryptosystems, The College Mathematics Journal, (1987, January, Volume 18.

[6] Gustavus J. Simmons, Symmetric and Asymmetric Encryption, Sandman Laboratories, Albuquerque, New Mexico 87185.

[7] KetuFile White Papers, Symmetric vs. Asymmetric Encryption, 2003-2004.

[8] U.S. Department of commerce/National Institute of Standards and Technology, Data Encryption Standard (DES), (1999, October, 25).

[9] Proceedings of the IEEE, VOL. 76, NO. 5, The First Ten Years of Public-Key Cryptography, May 1988.

[10] Randall J. Easter and Carolyn French, Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, (2012, May, 30).

[11] FIPS 197, Announcing the Advanced Encryption Standard (AES), 2001, November, 26.

[12] Adam Berenet, Advanced Encryption Standard by Example v.1.7, ABI Software Development.

[13] Evgeny Milanov, The RSA Algorithm, 2009, June, 03.

[14] Steven M. Bellovin and Eric K. Rescola, Deploying a New Hash Algorithm, Columbia University, 2005. Available: https://www.cs.columbia.edu/~smb/papers/new-hash.pdf.

[15] Chris Brooks, "Computers and Society, Introduction to Encryption, Department of Computer Science, University of San Francisco.

INDEKS AUTORA

CIP - Каталогизација у публикацији
Национална библиотека Црне Горе, Цетиње

ISBN 978-86-85775-15-4
COBISS.CG-ID 24749840

ISBN 978-86-85775-15-4