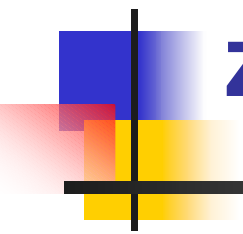


Zasebnost in nadzor na internetu, 3. del

Matej Kovačič,
http://www.ljudmila.org/matej

VARSTVO ZASEBNOSTI NA INTERNETU

- Zakonodajno in tehnično varstvo.
- Pot podatkov in teritorialna pristojnost zakonodaje (tržna inšpekcija - spam, udba.net).
- Varnost kot proces, varnostna kultura.
- Nekatere tehnike onemogočijo tako nezakonitega, kot tudi zakonitega prisluškovalca.

VARSTVO ZASEBNOSTI NA INTERNETU

- **Anonimizacija**.
- Popolna anonimizacija ni možna (razen z vključitvijo preko brezžičnega ali mobilnega omrežja).
- Uporaba "remailerjev" za pošiljanje pošte.
- Uporaba proxya in anonimnega proxya (web-based (SSL), standalone).
- Blokiranje piškotkov, selektivno blokiranje piškotkov (third-party, za določeno stran,... Mozilla).

VARSTVO ZASEBNOSTI NA INTERNETU

- **Zaščita pred prestrezanjem - šifriranje**.
- Kriptologija **- veda o tajnosti, šifriranju, zakrivanju sporočil (***kriptografija***) in o razkrivanju šifriranih podatkov (***kriptoanaliza***). *Kryptos logos* v grščini pomeni skrita beseda. Uporabljata se še pojma enkripcija (*šifriranje*) in dekripcija (*dešifriranje*). Osnovno sporočilo ponavadi imenujemo** čistopis **(*cleartext, plaintext*), zašifrirano pa** šifropis **ali** tajnopis **(*kriptogram, ciphertext*).**
- **Sporočilo po nekem** postopku **(*algoritmu, metodi*) spremenimo v kriptirano sporočilo, pri tem uporabimo določene vrednosti za parametre v algoritmu, ki jim rečemo** ključ**. Sogovornika se morata torej dogovoriti** o algoritmu in ključu**, da si lahko pošiljata šifrirana sporočila.**

ŠIFRIRANJE - primer

Primer šifriranja besede "INTERNET"

- **a -> a+1 po modulu 25:**
  JOUFSOFU
- **PGP:**

```
-----BEGIN PGP MESSAGE-----
Version: PGP Personal Security 7.0.3

qANQR1DBwU4DSfeOJ5LXyx4QCADL1H+hJPOSTwCVqDkzHv1fwzwL3V5vOegelXOg
SH/HF3qlCkhgfK4Qa2gp7SBuoXVenfY7vEzmCFLekc9ZJWgrtiyo9oVN6jzyBPgf
JmicJTBzrVAGY/CdS5F/N66e/KgVxfNGJo4oHxQWGdvyi/p4AayQMdV0RzQeWxZk
9t1Yp0bDD08dM0xEgm190ZUlBwgwY7LLnZd+la+DWeLoZmf8D4LUwq/bNNmVCH0Z
TkQY7fis4X9bYqFnpHodtkbgyN3/SE0sdE4rOVxHyKcVcgVrCbhFrnUMj+c1/XVA
ELiHA8JGQc+W1Rxs5sBQ9uBvnOAoB4/6t4JyrgPFtyOL9bUmCAD0ta+kLHVXWZLZ
1dMVl2CnHzTXxV6LdcQRrGhOU1J+9rtAZlMNdKUuoTwgH1ReFRAy3hSQYxaVrSul
4qj2Mt+Vm0KY1sXTFGZGCJZVrWeLWNtSr2kU02h6j9kBLR7LwvHwA2/LZ+yRDB/c
NMHhSGm9qghkKr9rpEqc+fpMNXxvBTiRcM9YFNhvLA6xaWJmtcH/+xLmQdeci4on
bV1ZbUgVtCKFmvIzI+4WRRlZXi7ndB0PanhGhThQwa0R/n+Hgx5iVUNVrJf2Nz19
/LaAuF93aEdIxGdn6hqttxd5weLQI9DMXGiuvYBVHAtpoCcQ1TWBJ1umulxhpEGt
eJJrXjXlyWwgehYpDAPAJn4rU5BUH3ca1C58AnSk6pACwZiT8Vk4w5u2skiTp1Gc
Fs3tRApGtQCEcn1Ea8fQ415qfO23WjPgv3w7OjGEC9ZV84ac0uRRTQECgFY3w4g/
PGIKlYMK2bBqzb6t70XwGo2YOsY=
=Dim8
-----END PGP MESSAGE-----
```

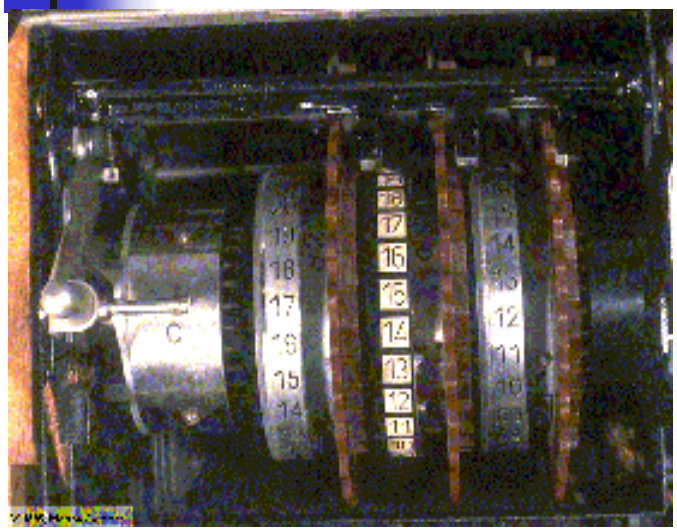
ŠIFRIRANJE - zgodovina

- Julij Cezar je svojim vojskovodjem pošiljal sporočila, kjer je vsako črko zamenjal s črko, ki je bila v abecedi nekaj mest za njo. Postopek lahko opišemo kot *zamenjavo črk a -> a+k po modulu 25* (tu smo metodo priredili za slovensko abecedo s 25 črkami). "k" predstavlja ključ. Cezar je menda običajno uporabil ključ 3.

C → F ; E → H ; Z → B; A → D; R → T

CEZAR → FHBDT

ŠIFRIRANJE - zgodovina



Nemci so med drugo svetovno vojno uporabljali šifrirne stroje Enigma. Tak stroj so sestavljali baterija, tipke za črke kot pri pisalnem stroju, luči za vsako črko in šifrirni mehanizem iz štirih okroglih ploščic (velikih kot plošček pri hokeju), ki so jih imenovali rotorji.

- Vojak je sporočilo šifriral tako, da je vtipkal posamezno črko in zapisal črko, ki se mu je osvetlila. Za presledke je vtipkal črko Z, števila pa je vtipkal z besedami. Naslovnik šifriranega sporočila je moral imeti stroj z enakimi rotorji (letalstvo je imelo svoje kombinacije, mornarica svoje,...). Spreminjali so tako začetne položaje rotorjev kot njihov vrstni red.

- **Nemci so menili, da tako kriptiranih sporočil ni mogoče dešifrirati, Angležem pa je to uspelo pod vodstvom Alana Turinga.**

VARNOST INFORMACIJ

- **Varnostna aplikacija mora zagotoviti naslednje:**
  - **zaupnost (*confidentiality*);**
  - **celovitost (*integrity*);**
  - **overjanje (*authentication*);**
  - **preprečevanje tajenja (*nonrepudiation*);**
  - **kontrolo dostopa (*access control*).**
- **To zagotovimo s podpisovanjem sporočil (*digital signitures*) in overjanjem javnih ključev. Sporočilu pa lahko dodamo tudi potrdilo (*certificate*), ki vsebuje še čas nastanka, podatke o lastniku, rok veljavnosti ipd.**
- **Če hočemo zagotoviti verodostojnost svojega sporočila, mu dodamo digitalni podpis: z zgostitvenim algoritmom izračunamo "prstni odtis" sporočila, ki ga zašifriramo s svojim zasebnim ključem. Prejemnik bo najprej z našim javnim ključem dešifriral podpis, iz sporočila bo ponovno izračunal "prstni odtis" ter ga primerjal s tistim, ki ga je dobil v podpisu. Če je sporočilo prišlo do njega nespremenjeno, se oba "prstna odtisa" ujemata.**

ŠIFRIRANJE - algoritmi

- **Pri varovanju podatkov uporabljamo** simetrične, asimetrične in zgostitvene **algoritme.**

- Simetričnimi algoritmi **ali algoritmi z zasebnim ključem: imamo samo en ključ, s katerim zašifriramo in dešifriramo sporočilo. Običajno so ti algoritmi hitri, težko pa je varno izmenjati ključ. Problem predstavlja tudi število ključev - vsak uporabnik mora imeti za vsakega dopisovalca svoj ključ.**

- Asimetrični algoritmi **ali algoritmi z javnim ključem: uporabnik ima dva ključa, enega objavi, drugi ostane tajen. Vsi, ki mu hočejo poslati sporočilo, bodo uporabili njegov javni ključ za šifriranje sporočila. Dešifriral pa ga bo lahko le on sam s svojim tajnim ključem in javnim ključem pošiljatelja. Te metode so računsko bolj zahtevne in zato počasnejše kot simetrične.**

- Zgostitveni algoritmi **poljubno dolg tekst preslikajo v število fiksne dolžine, kar je uporabno za digitalni podpis. Najbolj znana algoritma sta MD5 in SHA.**

ŠIFRIRANJE – varnost algoritmov

- **Kdaj je algoritem varen? Bistveno je, da je algoritem javno objavljen in da so ga imeli možnost preizkusiti vodilni kriptoanalitiki.**
- **Napad s preizkušanjem vseh možnih kombinacij bitov ključa (*brute-force attack*).**
- **Kako izbrati varno geslo, napad s slovarjem (*dictionary attack*), napad v primeru znane dolžine ključa.**
- **Analiza prometa med posameznimi vozlišči.**
- **Martin Gardner je avgusta 1977 v reviji Scientific American objavil 129 številk dolgo število in ponudil 100 dolarjev za razbitje na faktorje. Uganko je rešila mednarodna skupina z več kot 600 prostovoljci jeseni 1994.**
- **Leta 1999 pa so uspeli faktorirati 155-mestno število (kar ustreza 512 bitom). Zato je priporočljivo uporabljati daljše ključe od 512 bitov. RSA Security priporoča ključ 768 bitov za osebno uporabo, 1024 bitov za uporabo v organizacijah in 2048 bitov za ključe v izredno pomembnih operacijah.**

ŠIFRIRANJE – simetrični algoritmi

- **Delimo jih na dve skupini:**
  - **algoritmi za tekoče šifriranje (*stream ciphers*): sporočilo šifriramo bit za bitom;**
  - **algoritmi za šifriranje blokov (*block ciphers*): sporočilo razbijemo na bloke in vsak blok posebej šifriramo.**
- **Pri prvem načinu šifriramo tako, da kombiniramo bit ključa in bit sporočila. Če uporabimo kratek, ponavljajoč ključ, postopek ni varen - s kombiniranjem zašifriranega teksta je razmeroma lahko ugotoviti najprej dolžino ključa, potem vrednost ključa in nato dešifrirati sporočilo. Nasprotno pa je ta sistem nezlomljiv, če se ključ ne ponavlja in je povsem naključen niz bitov (*one-time pad*), vendar je velik problem kako zagotoviti naključnost.**
- **Večina algoritmov, ki jih danes uporabljamo v civilnih organizacijah, je blokovnih: sporočilo razbijemo na tako dolge bloke, in vsak blok preoblikujemo in kombiniramo s ključem. Zagotoviti je potrebno, da so v izhodnem bloku zabrisani vsi vzorci iz vhodnega bloka - skratka, da izgleda kot naključen niz bitov. Za vse dobre simetrične algoritme velja, da se izhoda ne da kompresirati za več kot nekaj odstotkov.**

ŠIFRIRANJE – simetrični algoritmi

- **Najbolj znani simetrični algoritmi so:**
  - **DES ali DEA (Data Encryption Standard/Algorithm), ki sta ga razvila NIST (National Institute of Standards and Technology) ter IBM;**
  - **RC2, RC4, RC5 - je razvil Ronald Rivest. RC4 je tekoč šifrirni algoritem z variabilno dolžino ključa do 2048 bitov. Vgrajen je v brskalnike kot del protokola SSL oziroma TLS, uporablja pa 128-bitni ključ;**
  - **IDEA (International Data Encryption Algorithm): razvila sta ga James L.Massey in Xuejia Lai v Zuerichu;**
- **Ameriška organizacija za standarde NIST je septembra 1997 razpisala natečaj za naslednika algoritma DES. Izmed 15 kandidatov so se v finale uvrstili naslednji algoritmi, ki so vsi uspešno prestali testiranja:**
  - **MARS (IBM)**
  - **RC6 (RSA Laboratories)**
  - **Rijndael (Joan Daemen, Vincent Rijmen)**
  - **Serpent (Ross Anderson, Eli Biham, Lars Knudsen)**
  - **Twofish (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson)**
- **Postopek za izbiro AES (Advanced Encryption Standard) je bil zaključen 2. oktobra 2000, ko je bil izbran algoritem** Rijndael**.**

ŠIFRIRANJE – asimetrični algoritmi

- **Asimetrični algoritmi za šifriranje uporabljajo drugačen ključ kot za dešifriranje.**
- **Asimetrični algoritmi se uporabljajo za izmenjavo skupnih ključev in za digitalno podpisovanje, za masovno šifriranje podatkov pa ne, ker so počasnejši od simetričnih algoritmov.**
- **Asimetrični algoritmi uporabljajo za šifriranje tako transformacijo, za katero je težko ali nemogoče izvesti inverzno transformacijo, če nimamo dodatne informacije oz. zasebnega ključa.**
- **Za take transformacije se uporablja izraz *One-Way Function* oziroma *Trap-door one-way function*: če imamo neko dodatno informacijo (trap-door, zasebni ključ) je inverzna operacija lahka, sicer pa skoraj nemogoča.**

ŠIFRIRANJE – asimetrični algoritmi

- **Prvi znani algoritem z javnim ključem za šifriranje podatkov je Merkle-Hellmanova metoda z nahrbtniki, vendar ni več v uporabi.**
- **Danes se najbolj uporablja algoritem RSA, razvit leta 1977, ki ima ime po svojih avtorjih (Ronald Rivest, Adi Shamir, Leonard Adleman). Metoda je v ZDA patentirana. Ker pa je bil opis metode objavljen pred vložitvijo zahtevka za patent, lahko RSA uporabljajo brez licenčnine povsod po svetu, razen v ZDA.**
- **Asimetrični algoritmi, ki temeljijo na eliptičnih krivuljah (*ECC - Elliptic Curve Cryptosystems*). Ideja je znana že od leta 1985. V primerjavi z RSA zadoščajo krajši ključi, zato kaže, da bodo v bodočnosti ti algoritmi prevladali.**
- **Diffie-Hellman: postopek za izdelavo in izmenjavo skritega ključa po javnem omrežju**
- **ElGamal: digitalni podpis, enkripcija**
- **RSA: digitalni podpis, enkripcija**
- **ECC: digitalni podpis, enkripcija**

ŠIFRIRANJE – primeri uporabe

- Enkripcija, dekripcija in digitalno podpisovanje elektronske pošte in datotek.
- PGP disk.
- Zakon o kazenskem postopku: 5. člen določa, da obdolženec ni dolžan pričati proti sebi ali svojim bližnjim ali priznati krivde.
- Steganografija - skrivanje sporočil, nevidno kodiranje, označevanje datotek z digitalnim vodnim tiskom ter digitalnimi serijskimi številkami.

VARSTVO ZASEBNOSTI NA INTERNETU

- **Zaščita pred vdori in zasegom podatkov**.

- Redno nameščanje porpavkov (WindowsUpdate).
- Protivirusni programi.
- Požarni zid.
- Šifriranje datotek in diskovnih pogonov.

VARSTVO ZASEBNOSTI NA INTERNETU

- **Brisanje elektronskih sledi**.
- Brisanje zunaj sistema (anonimizacija) je omejeno.
- Brisanje sledov uporabe računalnika:
  - Metoda mikroskopiranja magnetnih sil in trajno brisanje (wiping, number of passes).
  - Brisanje "swap datoteke".
  - Brisanje medpomnilnikov, piškotkov in lokalnih datotek aktivnosti.

VARSTVO ZASEBNOSTI NA INTERNETU

- **Zaščita pred tempest napadi**.
- Oklaplanje s kovino.
- Nadgraditev gonilnikov.
- Uporaba posebnih tempest pisav (tempest prevention font).