

Hyrje në kriptografi

Hyrje

Faton Berisha



Fakulteti i Shkencave Kompjuterike
Universiteti i Prizrenit

Qëllimet dhe objektivat

- Hyrje në kursin
- Kriptografia historike

Përmbajtja

- 1 Hyrje në kursin
 - Referenca të dobishme për kursin
- 2 Qëllimet dhe konfigurimet
 - Skemat kriptografike
- 3 Ç'është kriptografia

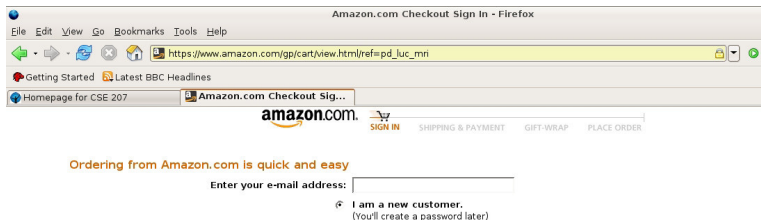
Referenca

- <http://www.fberisha.org>
- M. Bellare, P. Rogaway, *Introduction to modern cryptography*, University of California, 2015.
<http://cseweb.ucsd.edu/~mihir/cse107>
- J. Katz, Y. Lindell, *Introduction to modern cryptography*, CRC Press, 2014.
- R. Pass, A. Shelat, *A course in cryptography*, Cornell University, 2010.
<https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf>

Përdorimi i kriptografisë

- A e keni përdorur kriptografi?
 - Sot?
 - Gjatë javës së fundit?
 - Këtë vit?

Përdorimi i kriptografisë (Vazhdim)

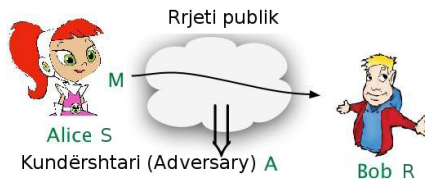


- https invokon protokolin e sigurisë së komunikimit Secure Socket Layer (SSL) për të bartur në mënyrë të sigurt numrin e kartelës suaj kreditore te serveri.
- SSL përdor kriptografi

Përdorimi i kriptografisë (Vazhdim)

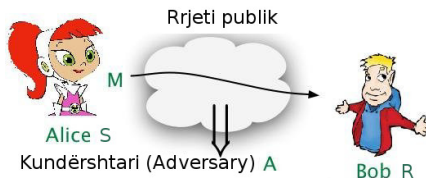
- Përdorime tjera të kriptografisë:
 - ATM makinat
 - Bankingu on-line (e-banking)
 - Autentifikimi në GMail
- Mbi 11,000 aplikacione Androidi përdrojnë kriptografi (enkriptim), dhe mbi 10,000 e bëjnë gabimisht.

Ç'është kriptografia?



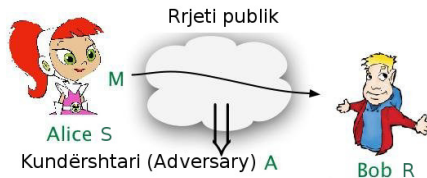
- Kundërshtati (Adversary A): person i zgjuar me kompjuter të fuqishëm
- Qëllimet (aspektet e sigurisë):
 - konfidencialiteti i të dhënave
 - integriteti dhe autenticiteti i të dhënave

Konfidencialiteti



- Qëllimi është që kundërshtari të mos i shohë ose marrë të dhënat (mesazhin) M
- **Shembull:** M mund të jetë numri i kartelës kreditore që dërgohet nga blerësja Alice te serveri Bob dhe ne dëshirojmë të sigurojmë se kundërshtari A nuk e mëson atë.

Integriteti dhe autenticiteti



- Qëllimi është që të sigurohet se:
 - M vërtet ka origjinën nga Alice dhe jo dikush tjetër,
 - M nuk është modifikuar gjatë bartjes.

Shembull integriteti dhe autenticiteti

Alice

Bob
(Banka)

Alice
Paguaj 100 € Charlie-t



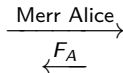
- Qëllimi është që të sigurohet se:
 - Kundërshtari Eve nuk do të mund të:
 - Modifikonte „Charlie“ në „Eve“
 - Modifikonte „100 €“ në „1000 €“
- Integriteti eviton sulmet e tilla.

Bazat mjekësore të të dhënave

Doktori

Lexon F_A

Modifikon F_A në F'_A



Baza e të dhënave

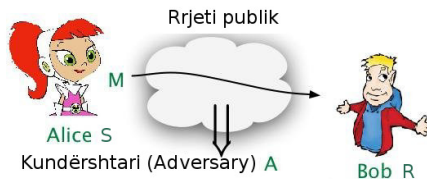
Alice	F_A
Bob	F_B



Alice	F'_A
Bob	F_B

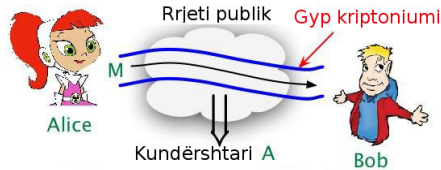
- Konfidencialiteti: F_A , F'_A përmbajnë informatë private dhe dëshirojmë të sigurohemi se kundërshtari nuk do t'i marrë
- Integriteti dhe autenticiteti: Duhet siguruar
 - doktori është i autorizuar të marrë fajlin e Alice-ës
 - F_A , F'_A nuk modifikohen gjatë bartjes
 - F_A vërtet është dërguar nga baza e të dhënave
 - F'_A vërtet është dërguar nga doktor (i autorizuar)

Ç'është kriptografia?



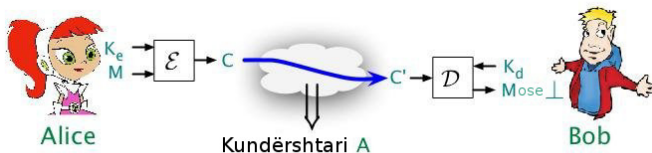
- Kundërshtati (Adversary A): person i zgjuar me kompjuter të fuqishëm
- Qëllimet
 - Konfidencialiteti i të dhënave
 - Integriteti dhe autenticiteti i të dhënave

Bota ideale



- Kanal ideal (Gyp kryptoniumi): Nuk mund të shikohet brenda ose të ndryshohet përmbajtja.
 - Do të arriheshin të gjitha qëllimet tona!
 - Por kryptoniumi gjendet vetëm në planetën Krypton dhe është me mungesë oferte. 😞

Skemat kriptografike

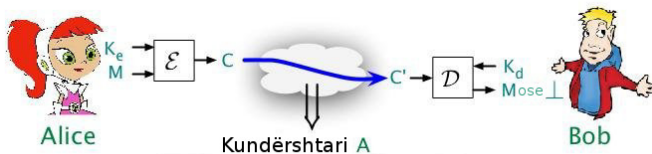


\mathcal{E} : algoritëm enkriptimi K_e : çelës enkriptimi

\mathcal{D} : algoritëm dekriptimi K_d : çelës dekriptimi

- Algoritmat: Të standardizuar, të implementuar, publikë!

Skemat kriptografike (Vazhdim)



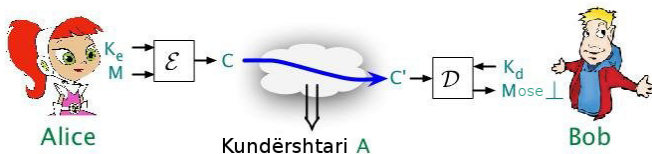
\mathcal{E} : algoritëm enkriptimi K_e : çelës enkriptimi

\mathcal{D} : algoritëm dekriptimi K_d : çelës dekriptimi

- Konfigurimet:**

- **Çelës privat (simetrik):** $K_e = K_d$ sekret
- **Çelës publik (asimetrik):** K_e publik, K_d sekret

Skemat kriptografike (Vazhdim)



\mathcal{E} : algoritëm enkriptimi

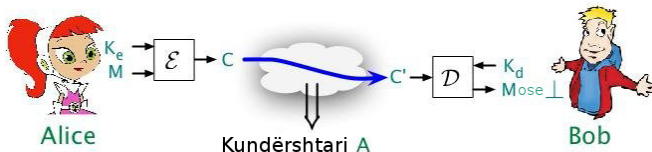
K_e : çelës enkriptimi

\mathcal{D} : algoritëm dekriptimi

K_d : çelës dekriptimi

- Si shpërndahen çelësat?
 - Magji, tani për tani!

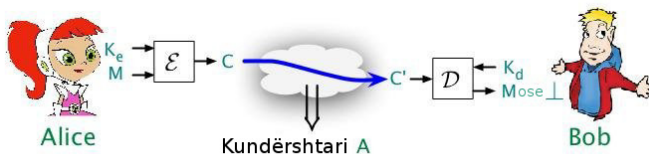
Skemat kriptografike (Vazhdim)



- Problemet tona:

- Si t'i përkufizojnë qëllimet e sigurisë?
- Si t'i dizenojmë \mathcal{E} , \mathcal{D} ?
- Si kemi besim se \mathcal{E} , \mathcal{D} arrijnë qëllimet tona?

Skemat kriptografike (Vazhdim)



- **Siguria kompjuterike:** Si kompania/sistemi mbron K_E/K_D nga thyerja (virusë, worms, vrimat në SO, ...)?
- **Kriptografia:** Si i shfrytëzojmë K_E , K_D për të siguruar komunikim të sigurtë nëpër një rrjet të pasigurtë?

Pse është kriptografia e vështirë?

- Nuk mund të anticipohet paraprakisht strategjia e një kundërshtari; numri i mundësive është i pafundëm.
- „Testimi“ është i pamundur në këtë konfigurim.

Histori e hershme

- Shifruesit me zëvendësim/shifruesit Caesar

$$K_e = K_d = \pi : \Sigma \rightarrow \Sigma, \quad \text{një permutacion sekret.}$$

P.sh., $\Sigma = A, B, C, \dots$ dhe π është si në vijim:

σ	A	B	C	D	...
$\pi(\sigma)$	E	A	Z	U	...

$$\begin{aligned} \mathcal{E}_\pi(\text{CAB}) &= \pi(\text{C})\pi(\text{A})\pi(\text{B}) \\ &= \text{ZEA} \end{aligned}$$

$$\begin{aligned} \mathcal{D}_\pi(\text{ZEA}) &= \pi^{-1}(\text{Z})\pi^{-1}(\text{E})\pi^{-1}(\text{A}) \\ &= \text{CAB} \end{aligned}$$

- Nuk është shumë e sigurtë! (Rebus gazetash)

Koha e makinave

- Enigma: Makinë gjermane e Luftës II Botërore



- E thyer nga anglezët në një përpjekje të udhëhequr nga Alan Turing.

Enkriptimi i Shannon dhe One-Time-Pad (OTP)

- K zgjedhet në mënyrë të rastësishme nga $\{0, 1\}^k$

$$K_e = K_d = K \xleftarrow{\$} \{0, 1\}^k$$

- Për çdo $M \in \{0, 1\}^k$
 - $\mathcal{E}_K(M) = K \oplus M$
 - $\mathcal{D}_K(D) = K \oplus C$



Teoremë (Shanon)

OTP është perfekt (i përkryer) i sigurtë përderisa enkriptohe vetëm një mesazh (d.m.th. në qoftë se $|M| = |K|$).

- Fshehtësi „perfekte“, nocion i definuar nga Shannon, kap pamundësinë matematike për të thyer një skemë enkriptimi.
- Fakt: Në qoftë se $|M| > |K|$, atëherë asnjë skemë nuk është perfekt e sigurtë.

Kriptografia moderne: Shkencë kompjutative

- Siguria e një sistemi „praktik“ duhet të mbështetet jo në pamundësinë por në *vështirësinë kompjutative* të thyerjes së sistemit.
 - „Praktik“: më tepër bit mesazhi sesa bit çelësi ($|M| > |K|$).
- Në vend se të themi „Është e pamundur të thyhet skema“...
- Do të mund të ishim në gjendje të themi „Asnjë sulm me kompleksitet $\leq 2^{160}$ ($= t$) ka sukses me probabilitet $\geq 2^{-20}$ ($= \frac{t}{2^{200}}$)“.
 - D.m.th., sulmet mund të ekzistojnë përderisa kostoja për ngritjen e tyre është parandaluese.
 - Kosto: koha e kompjutimit, memoria kompjuterike, \$\$\$.

Kriptografia moderne: Shkencë kompjutative (Vazhdim)

- Siguria e një sistemi „praktik“ duhet të mbështetet jo në pamundësinë por në *vështirësinë kompjutative* të thyerjes së sistemit.
- Kështu, kriptografia nuk është vetëm matematikë; mbështetet poashtu në shkencën kompjuterike:
 - Teorinë e kompleksitetit të kompjutimit
 - Disenjin dhe analizën e algoritmave

Problemi i faktorizimit

Shembull

Gjeni faktorët e thjeshtë të numrit 85.

Zgjidhje

$$85 = 5 \cdot 17$$

Algoritëm Factor(N)

Input: Numri i përbërë N

Output: Faktori më i vogël i thjeshtë i N

for $i = 2$ to $\lfloor \sqrt{n} \rfloor$ **do**

if $N \bmod i = 0$ **then**

return i

end if

end for

Problemi i faktorizimit (Vazhdim)

- Shkruarja e programit për faktorizim: E thjeshtë!
- Por...



algoritmi është tepër i ngadalshëm...

- Parandaluese në qoftë se N është i madh (p.sh., 400 shifror).

A mund të faktorizojmë shpejt?

- Si të faktorizojmë shpejt?

- Gauss-i nuk arriti ta gjente si
- Askush sot nuk di si



- Askush sot nuk di si të faktorizohet një numër 400 shifror për një kohë praktike.
- Faktorizimi është një shembull problemi të vështirë kompjutues.

Primitivat ose problemet atomike

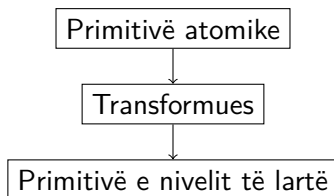
- Shembuj:
 - Faktotizimi: Për $N = pq$ të madh, gjeni p , q .
 - Primitivat blok shifruese: DES, AES, ...
 - Hash funksionet: MD5, SHA1, SHA3, ...
- Përparsitë:
 - Disa primitiva të tilla
 - Disenjimi art, besimi nga eksperiencia (historia).
- Mangësitë:
 - Nuk e zgjidhin drejtpërdrejt ndonjë problem sigurie.

Primitivat e një niveli më të lartë

- Qëllimi: Zgjidhja e problemit të sigurisë me interes të drejtpërdrejt.
- Shembuj: enkriptimi, autentifikimi, nënshkrimet digjitale, shpërndarje e çelësit, ...
- Përparsitë:
 - Të shumëta.

Qasja e mbindërtimit

- Tipikisht, ndërtojmë primitiva të nivelit të lartë nga primitiva atomike.



Përkufizimi i sigorisë

- Një masë e madhe disenji përpiqet të prodhojë skema pa bërë më parë pyetjen: „Çfarë është saktësisht qëllimi i sigorisë?“
 - Si rezultat, fitohen skema që janë komplekse, të paqarta dhe të gabuara.
- Aftësia për të formuluar saktësisht çfarë është qëllimi i sigorisë së një disenji është sfiduese por e rëndësishme.
 - Arsyeon shtjellimin dhe zhvillimin e nocionit të fortë, të saktë të sigorisë
 - Të menduarit sipas këtyre qëllimeve precize dhe të kuptuarit e nevojës për to është njëri nga qëllimet e kursit.

Përkufizimi i sigurisë (Vazhdim)

- Çfarë do të thotë që një skemë enkriptimi të ofrojë konfidencialitet?
- A do të thotë që për $C = \mathcal{E}_{K_e}(M)$ të dhënë, kundërshtari nuk mund të
 - kthejë M ?
 - kthejë bitin e parë të M ?
 - kthejë XOR të bitit të parë të M dhe bitit të fundit të M ?
 - ...
- Përkufizim formal i konfidencialitetit implikon të gjitha të mësipërmet (dhe më tepër).

Shfrytëzime të reja të matematikës së vjetër

- Kriptografia shfrytëzon
 - teorinë e numrave
 - kombinatorikën
 - algjebrën moderne
 - teorinë e probabilitetit
- Teoria e numrave është fundamenti i sistemeve moderne me çelës publik, si RSA.

Kriptografia përtej sigurisë së komunikimit

- Gjetja e ndonjë vlere të përbashkët, p.sh. mesatarës:
 - Palët $1, 2, 3, \dots, n$.
 - Pala i ka numrin $x_i \in \{0, 1, \dots, M-1\}$
 - Dëshirojnë ta dijnë

$$x = \frac{x_1 + x_2 + \dots + x_n}{n}$$

por secila palë i do ta mbajë privat numrin e vetë x_i .

- Përdorimi:
 - x_i : Rezultati i studentit i në provimin periodik
 - x_i : Vota e partisë i për një propozim të caktuar në një votim parlamenti
 - ...

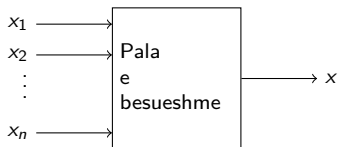
Kriptografia përtej sigurisë së komunikimit (Vazhdim)

- Palët 1, 2, 3, ..., n .
- Pala i ka numrin $x_i \in \{0, 1, \dots, M-1\}$
- Dëshirojnë ta dijnë

$$x = \frac{x_1 + x_2 + \dots + x_n}{n}$$

por secila palë i do ta mbajë privat numrin e vetë x_i .

- Zgjidhja me një palë të besueshme:



- Kompjutim i sigurtë: Lejon arritjen e objektivit pa palë të besueshme, duke zbatuar vetëm komunikim (të sigurtë) ndërmjet palëve.

Lojërat e fatit në Internet

Lojtari



$$\begin{array}{c} \xrightarrow{1 \text{ €}, g} \\ \xleftarrow{R, T} \end{array}$$

Kasino



$$T \xleftarrow{\$} \{1, \dots, 100\}$$

$$R \leftarrow \begin{cases} 200 \text{ € në qoftë se } g = T, \\ \text{😞 përndryshe} \end{cases}$$

- A do të luanit?
- Kasinoja mund të mashtrojë.
 - Të kthejë 😞, T për ndonjë $T \neq g$
- Kriptografia mund ta rregullojë këtë!

Kriptografia sot

- Miliona dollarë humbje për shkak të mashtrimeve me kartela kreditore, phishing, identity theft, . . .
- Mungesë konfidencialiteti: Sasi enorme informatash mbi secilin prej nesh mbledhet dhe shfrytëzohet nga biznese të dedikuara për këtë qëllim
- Mungesë konfidencialiteti: Informata mbi komunikime private të mbledhura nga agjenci të caktuara.
- Kriptografia është vegël qendrore në sigurimin e më tepër sigurie.

Kriptografia në botën reale

- Ekspozim i dobët: Specifikim jokomplet, i paqartë i skemës në dokumente
- Mungesë formulimi preciz i qëllimit
- Skema komplekse, të paqarta ose jokorrekte
- Pasojë e mungesës së arsimimit dhe shkathtësive kriptografike te fuqia punëtore.

Fillet e arsimimit kriptografik

- Arsimimi kriptografik do të duhej të ofronte aftësi për:
 - Identifikimin e kërcënimeve
 - Vlerësimin e zgjidhjeve dhe teknologjive të sigurisë
 - Disenjimin e zgjidhjeve kualitative
 - Shkruarjen e specifikimeve të qarta dhe complete të skemave
- Në mos asgjë tjetër, të zhvillojë një ndjesi të shëndoshë paranoje!