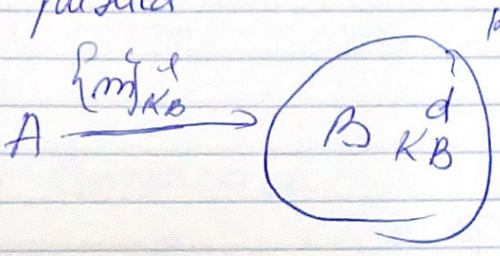
Subject : Date : ../../....

5.i. - curs 5 site git proiect

Criptografia cu chei publice

(pK, sK) privata
publica



~~##~~ RSA, ElGamal

RSA $\mathcal{O}((\log M)^3)$, determinist

$K_B^e = (n, e)$ $n = p \cdot q$

e inversabil mod $\phi(n) = (p-1)(q-1)$

$K_B^d = (p, q, d)$ $d = e^{-1} \bmod \phi(n)$

$c = \{m_{K_B}\} = m^e \bmod n$

minim de securitate 1024-bit

parametrul e poate fi mic

Subject :

Date : ...../...../.....

Daca randomizez msg în RSA atunci RSA ∈ IND-CPA

ElGamal randomizată decarece merge soluționat în $O(\log^3 p)$

$K_B^e = (p, g, g^a)$

p = numar prim

g = generator mod p

a secret

$K_B^d = (a)$

$g^a \rightarrow$ a problema dificilă

$E(m)_{K_B^e} = (g^e, m \cdot g^{ab})$

b alb la criptare

$c = (c_1, c_2) = (g^e, m \cdot g^{ab})$

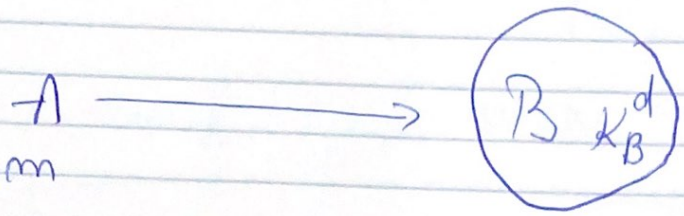
$g^{ab} = (g^a)^b$

Subject :

Date : ... / ... / ...

PKE = cripto sistem cu chei publice

PKE = poate fi de 1000 de ori mai lent decat SKE
cu chei simetrice



A Generează o cheie simetrică K

$c_1 = \{K\}_{K_B^e}$

$c_2 = \{m\}_K$

criptare hibridă

TLS, PGP, IPSec, S/MIME

In cazul criptării hibride, SKE poate avea securitate IND-CCA

Daca SYST PKE are IND CPA => sistemul hibrid are IND-CPA

Cu cat mesajul care se criptează este mai mic atunci criptarea este mai vulnerabilă

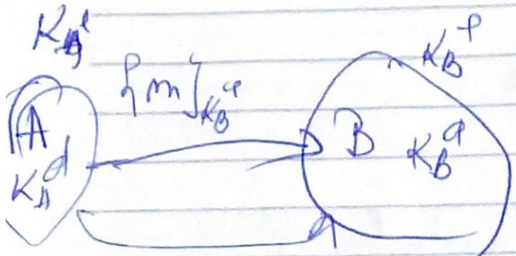
Subject :

Date : ..../..../.....

Semnături digitale

(PK, SK) → pt semnat SK

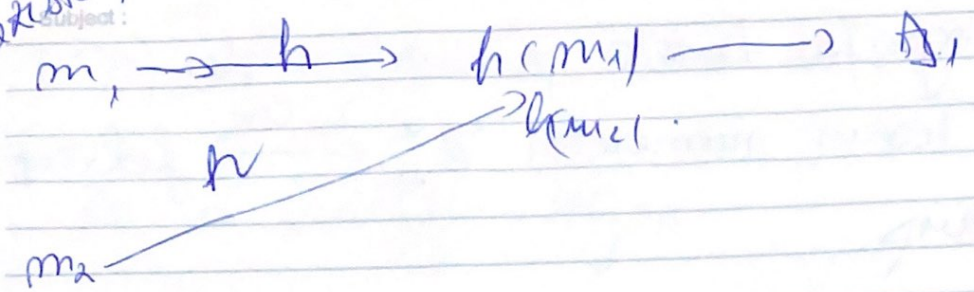
→ pt criptare PK



$m, \{m\}_{K_A}^d$

Semnătura de mână	Sem digitală
1. nu depinde de document	1. depinde de document
2. se atașează doc	2. nu se atașează doc.
3. se verifică în fct de semnătură	4. se verifică în fct de semnătură și de document
4. cheie de verificare secretă	4 are cheie de verificare publică
5. are dim mică indiferent de doc	

existența ca coliziune



$K \leftarrow \mathbb{Z}_{p-1}$ aleator

$m = a\gamma + K\delta \bmod p-1$

$\gamma = g^K \bmod p$ $\quad O(\log^3 K)$

$\delta = (m - a\gamma) K^{-1} \bmod p-1$

Cheia publică devine din ce în ce mai mare

Instanțe ușoare ale unei probleme grele pot fi rezolvate eficient

Subject :

Date : ..../..../....

Criptografia bazata pe curbe eliptice (ECC)

T.F = Teoria numerelor $\mathbb{Z}_n^*$ ←→ folosit alt grup

Prob dificila ←→ Prob dificila

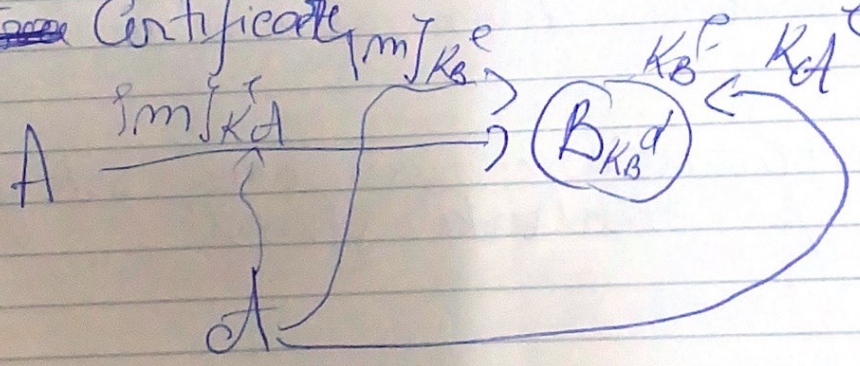
Acolo unde nu intelegeam curba acolo aveam pct la infinit

PLA $\quad \mathbb{Z}_p^*$

g^a

$a = ?$

~~Teorema~~ Certificate



sau da a certifica cheia publica

$C(B) = (ID(B), K_B^e, Info, Sig_{TA})$

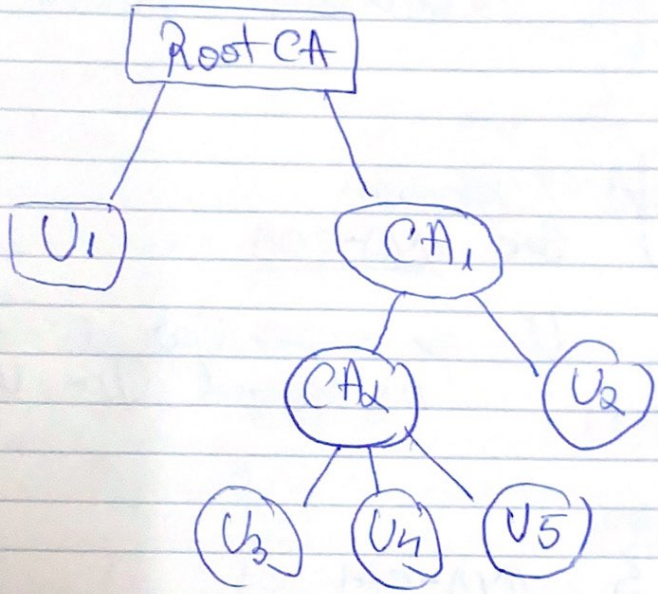
Subject :

Date : ../../....

X.509 = format slide 24

A va verifica sig_{TA}

↳ merge la cheie publica a lui TA pt verificare



Lant de incredere = lant de verif a certif.

Rev = ?

Management sist cu chei publice = PKI
Infrastructura pt lucru cu chei publice

Criptografie bazata pe identitate

IBARE = met. de schimb de chei bazate pe identitate