Institucioni i Arsimit
UNIVERSITAR AAB

PRISHTINË

FAKULTETI I SHKENCAVE KOMPJUTERIKE

FUNKSIONI HASH (FUNKSIONI PRERES)

1. Procese ku i ri-modelont dhenat ne dalje me gjatesi fikse

2. HASH funksionet jane nje-dimensional

Zbatimi i HASH:

- verifikimi i te dhenave – Shumica e algoritmeve te nenshkrimeve dixhitale jane te ndertuara ne baze te funksioneve HASH

- verifikimi i fjalekalimit – konsiston ne ruajtjen e funksionit HASH per cdo fjalekalim

HASH FUNKSIONET KRYESORE

Tipi	Emertimi	Bitet e Daljes	Bytet e Daljes
SHA 1	Security Hash Algorithm (update)	160 bit	20 byte
SHA 2	Security Hash Algorithm (update)	256 bit	32 byte
SHA 3	Security Hash Algorithm (update)	512 bit	64 byte
MD 4	Message digest 4	128 bit	16 byte
MD 5	Message digest 5	128 bit	16 byte
MD 6	Message digest 6	512 bit	64 byte

SHEMBULLI

Te shifrohet mesazhi:

"computer science at universiteti aab"

me funksionin preres (HASH) SHA1. (40 njesi / 160bit / 20byte)

computer	===>	Hash / SHA1	===>	8D99 9584 1B7F 8D22 79B7 A71B 6B78 AF87 53B2 3A8E
science	===>	Hash / SHA1	===>	8D99 9584 1B7F 8D22 79B7 A71B 6B78 AF87 53B2 3A8E
at	===>	Hash / SHA1	===>	27E9 0DFA 57C3 58AC FAF4 7086 0F6F 72C9 282C E995
university	===>	Hash / SHA1	===>	40B9 04FD 8852 297D AEAE B426 B1BC A46F D245 4AA3
aab	===>	Hash / SHA1	===>	F9F9 1406 0CCB 1E10 D551 AD49 016B 1A66 58D6 EDEC

SHEMBULLI

(HASH) SHA 2. (64njesi / 256bit / 32byte)

computer	===>	Hash / SHA2	===>	AA97 3021 50FC E811 425C D845 3702 8A5A FBE3 7E3F 1362 AD45 A51D 467E 17AF DC9C
science	===>	Hash / SHA2	===>	AD45 A51D 467E 17AF 23C8 AA97 3021 50FC E811 425C D845 3702 8A5A FBE3 7E3F FBE3
at	===>	Hash / SHA2	===>	17AF 23C8 AA97 3021 50FC E811 425C D845 3702 8A5A FBE3 7E3F 3021 BE3 7E3F FBE3
university	===>	Hash / SHA2	===>	FBE3 7E3F 3021 BE3 7E3F AA97 3021 50FC E811 425C D845 3702 8A5A FBE3 7E3F 50FC
aab	===>	Hash / SHA2	===>	D845 3702 8A5A FBE3 7E3F 3021 BE3 7E3F 3021 50FC E811 425C D845 3702 8A5A FBE3

SHEMBULLI

(HASH 3) SHA 3. (116njesi / 512bit / 64byte)

computer	===>	Hash / SHA3	===>	DBAF 470E 968C 60A3 1890 4E61 145C 6E4C 18BE 449F C891 661A 7445 F852 194F 48E4 13C8 A170 BA27 FC89 AE46 80A9 3AAF 3FEF
science	===>	Hash / SHA3	===>	923B 23B3 65CB 200C A988 F6F5 6882 F61A 6A68 A3BD CB90 5378 5E3A D621 7FF2 BF3A 6532 F65A E22E 73DD CFFA AF10 62E9 09DF
at	===>	Hash / SHA3	===>	200C A988 F6F5 6882 F61A 6A68 A3BD CB90 5378 5E3A D621 7FF2 BF3A 6882 F61A 6A68 A3BD CB90 5378 5E3A E22E 6532 F65A CB90
university	===>	Hash / SHA3	===>	470E 968C 60A3 1890 4E61 145C 6E4C 18BE 449F C891 661A 7445 F852 194F 48E4 13C8 A170 61A 6A68 A3BD BF3A 6532 F65A BF3A
aab	===>	Hash / SHA3	===>	A3BD CB90 5378 5E3A D621 7FF2 BF3A 6532 F65A E22E 6532 F65A A988 F6F5 6882 F61A 6A68 A3BD CB90 5378 449F C891 661A 7445

SHEMBULLI

(HASH) MD5. (32 njesi / 128bit / 16byte)

computer	===>	Hash / MD5	===>	DF53 CA26 8240 CA76 670C 8566 EE54 568A
science	===>	Hash / MD5	===>	FB5C 7F9B B4B3 2CE2 F3BF F466 2F1A B27B
at	===>	Hash / MD5	===>	7D0D B380 A5B9 5A8B A1DA 0BCA 241A BDA1
university	===>	Hash / MD5	===>	1023 8D61 1489 4BB5 EDC3 9981 835B BEC9
aab	===>	Hash / MD5	===>	E625 95EE 98B5 8515 3DAC 87CE 1AB6 9C3C

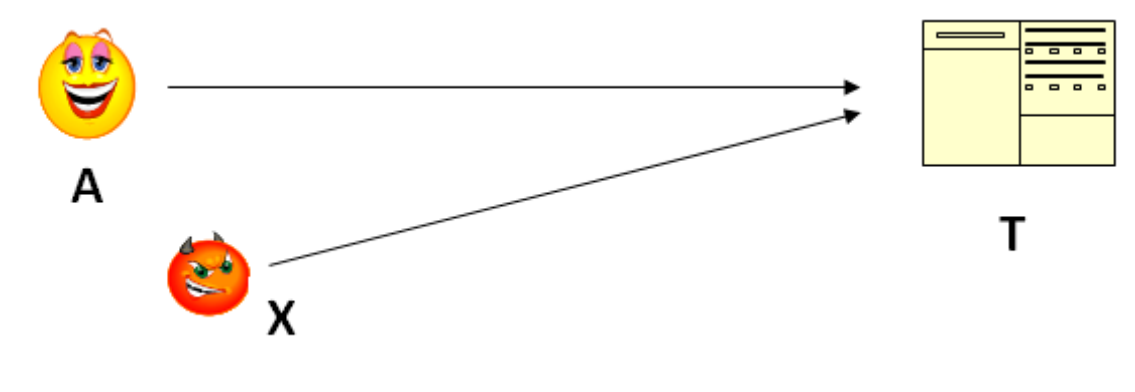
USER AUTHENTICATION

User Authentication
Proces i vertetimit te identitetit te perdoruesve per nje system te caktuar, e cila bazohet ne diqka individuale

User Authentication Protocol
Jane rregulla te procesit te vertetimit (identitetit) perdoruesve, kemi dy lloje:

- One Way (fjalekalimet)
- Two-way
  - Celes Simetrik (Nedham-Shreder, Kerberos)
  - Celes Publik (Dening-Sako, Wo-lam)

ONE WAY AUTENTICATION

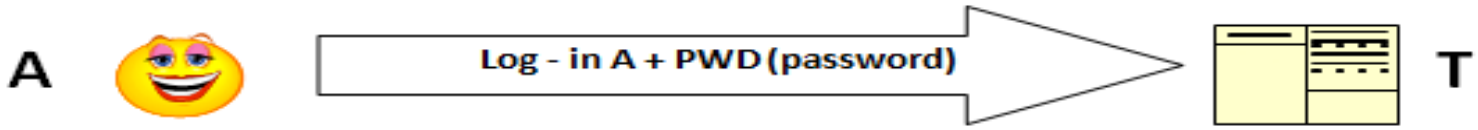


- Si mund te dije Host-i se eshte A-ja ajo qe do te kyqet dhe jo X-i?

- Problemi i teknikes One-Way!!!
  Hosti ruan te gjitha fjalekalimet ne menyre te paster

- Zgjidhja e problemmit: Funksionet One-Way dhe Sulmet-Fjalor

VERTETIMI PERMES FUNKSIONEVE HASH



User ID	H(pwd)
A	H_A
B	H_B
...	...

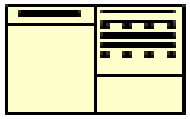
- Host nuk ka nevoje te dije fjalekalimin e A-se, por ka nevoje te dije vetem diferencen mes funksioneve HASH. Host konsiston nese H_A gjindet ne listen e H(pwd)

- **Sulmi duke perdorur nje fjalor** konsiston duke krijuar nje liste me fjalekalime te zakonshme dhe duke aplikuar mbi ate liste HASH funksione per cdo fjalekalim dhe nese pershtatet ndonji funksion, atehere gjejme fjalekalimin !!!

MBROJTJA NGA SULMET ME FJALOR

A

Log - in A + Fjalekalimi



T

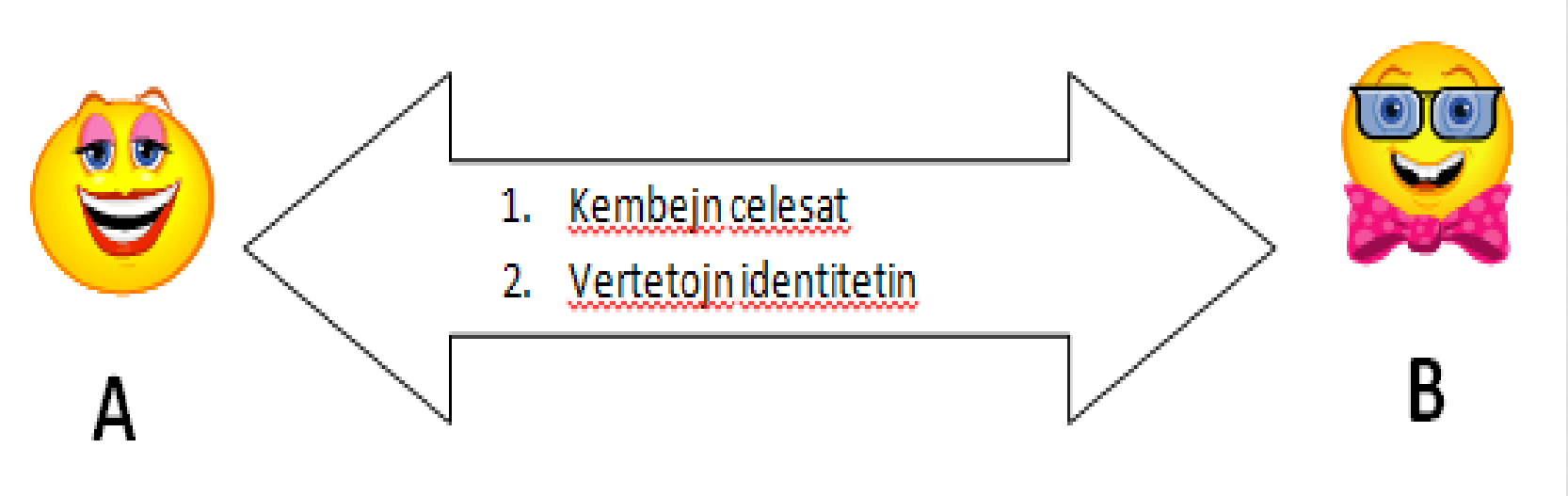
User ID	salt	H(pwd)
A	***	H_A
B	***	H_B
...	...	...

- sulmuesit nuk mund te perdorin te njejtin fjalor per ti thyer te gjitha sistemet me fjalekalime. Ha = H(S,pwd)

PERFUNDIME MBI FJALEKALIMIN

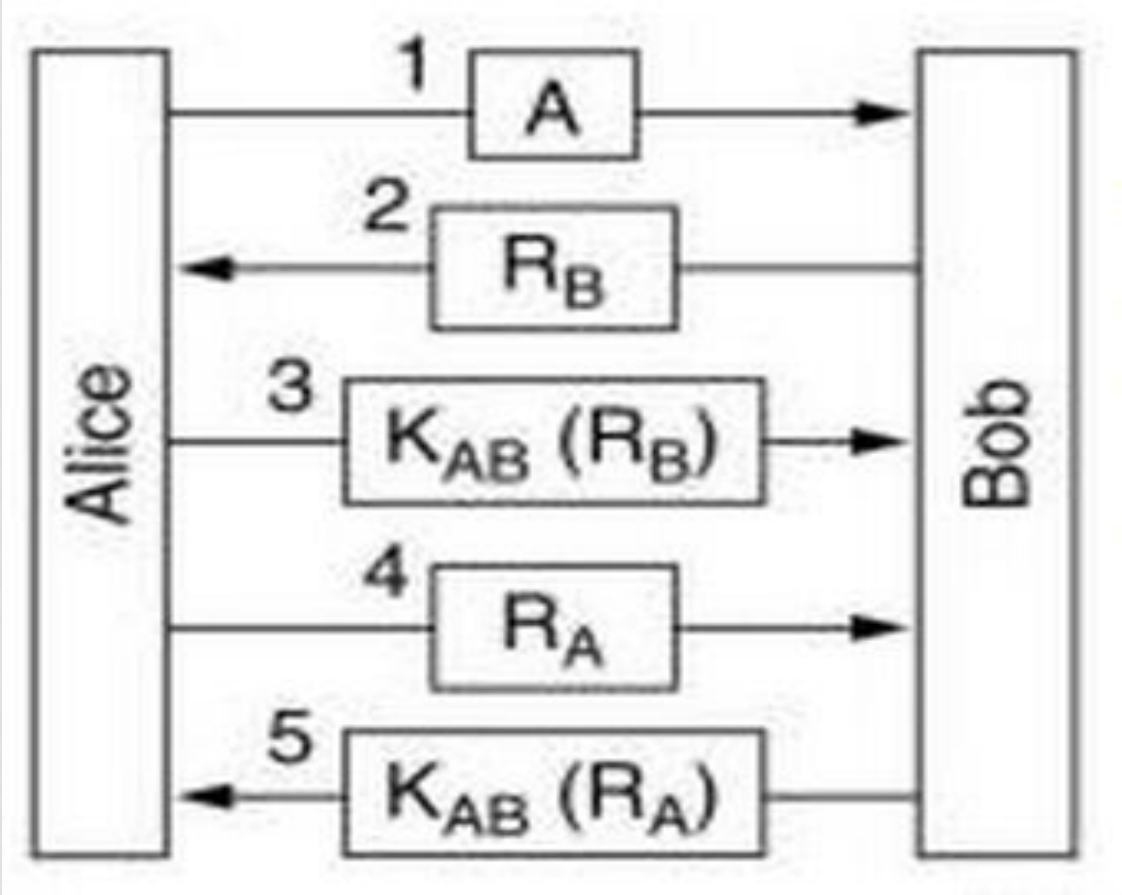
- Mos perdor asnjehere informacion personal
- Perdor kombinime fjale + karaktere + numra
- Mos e perdor te njejtin fjalekalim per shume sisteme
- Ndrysho falekalimin shpesh
- Perdor fraza:
  - Fjalekalimi im nuk eshte i lehte per tu thyer
  - FINEILPTTH

VERTETSIA DY-DIMENSIONALE



- Proces kur A dhe B identifikojne vertetsine e njeri tjetrit ne te njejten kohe dhe sigurohen qe po flasin mes vete.

VERTETESIA DUKE U BAZUAR NE CELESIN SEKRET TE PERBASHKET

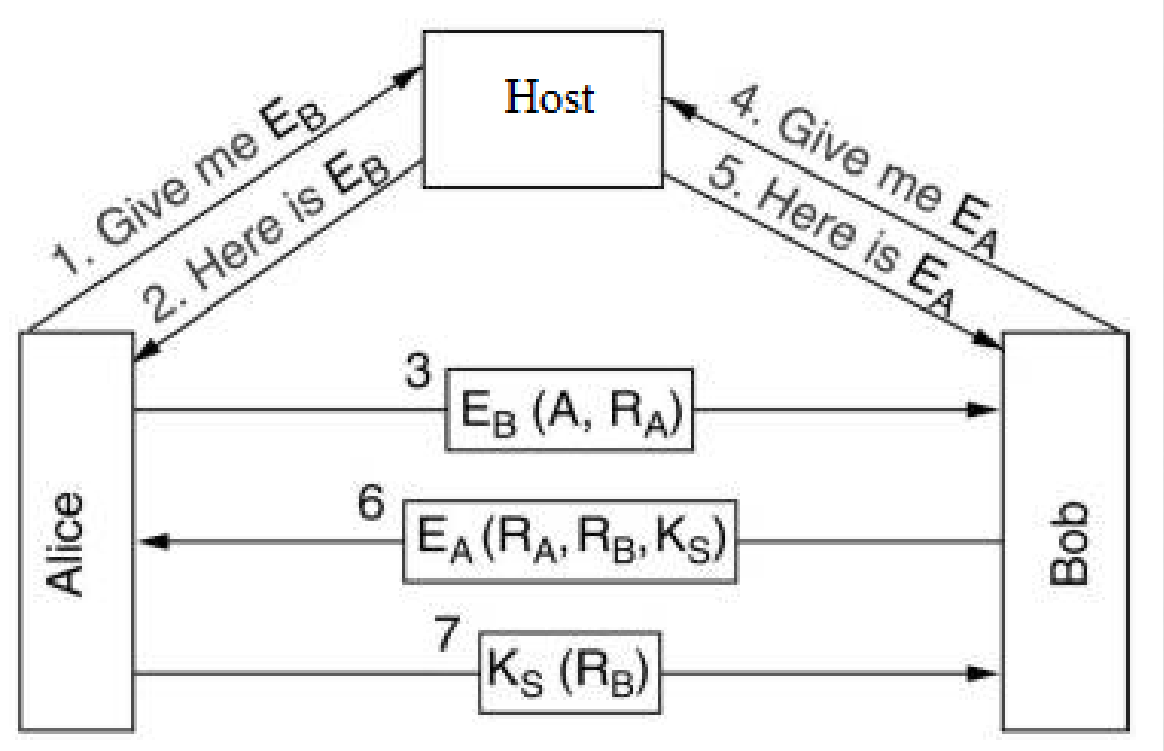


R = random nuber

A = identitet

K = celes

VERTETESIA DUKE U BAZUAR NE CELESIN PUBLIK



E = celesi publik

R = Random number

Ks = celes simetrik nje-perdorimesh

FALEMNDERIT

Pyetje?