Logika Autentikacije

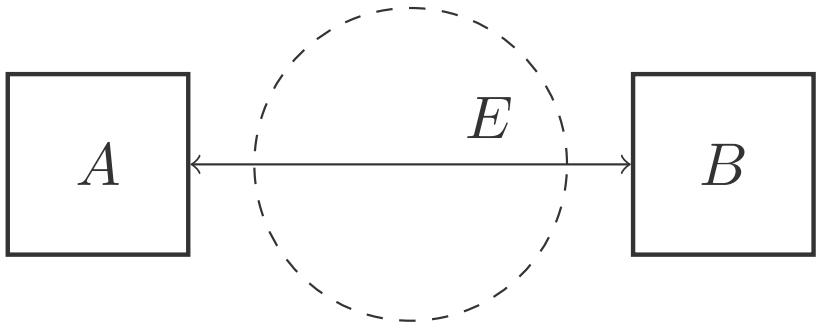
Momčilo Topalović

Matematička gimnazija
NEDELJA INFORMATIKE v5.0

17. decembar 2018.

Kriptografija

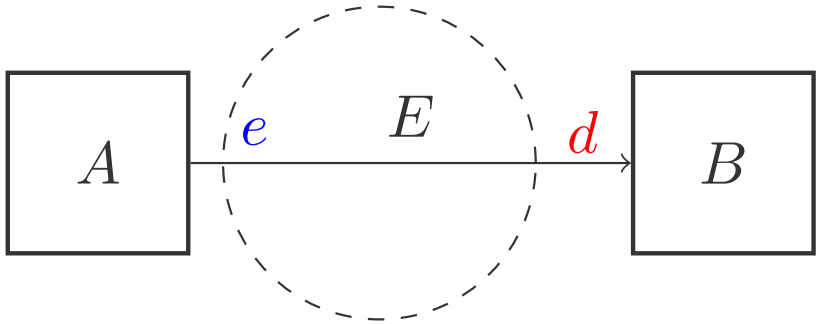
- Šta je kriptografija?



- Zahtevi protokolima
  - Tajnost (E ne može da rastumači poruke poslate između A i B)
  - Autentikacija (B je siguran da je poruka poslata od A stvarno od A)

Kriptografija javnog ključa

- Imamo dva ključa: privatni (d) i javni (e)



- d koristimo za dekripciju (dešifrovanje)
- e koristimo za enkripciju (šifrovanje)
- B izračunava i e i d
- Objavljuje e – svako može da posalje poruku B-u
- Ne objavljuje d – niko ne može da rastumači poruke poslane njemu

- $n = pq$, gde su p i q prosti
- $\phi = \varphi(n) = (p-1)(q-1)$
- $e: \quad (e, \phi) = 1$
- $d: \quad ed \equiv 1 \mod \phi$

Teorema (Ojler)

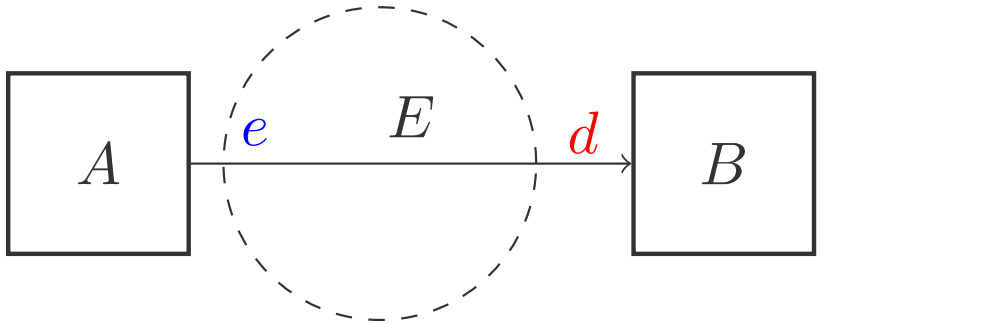
Za svako $m \in \mathbb{N}$ koje je uzajamno prosto sa n važi:

$$m^{\varphi(n)} \equiv 1 \mod n$$

- $m^{ed} \equiv_n m$

RSA

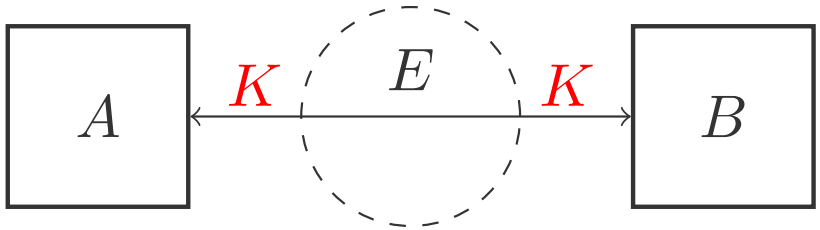
- (e, n) koristimo kao javni ključ
- (d, n) koristimo kao privatni ključ



$$m \xrightarrow{M = [m^e]_n} m = [M^d]_n$$

Symetrična kriptografija

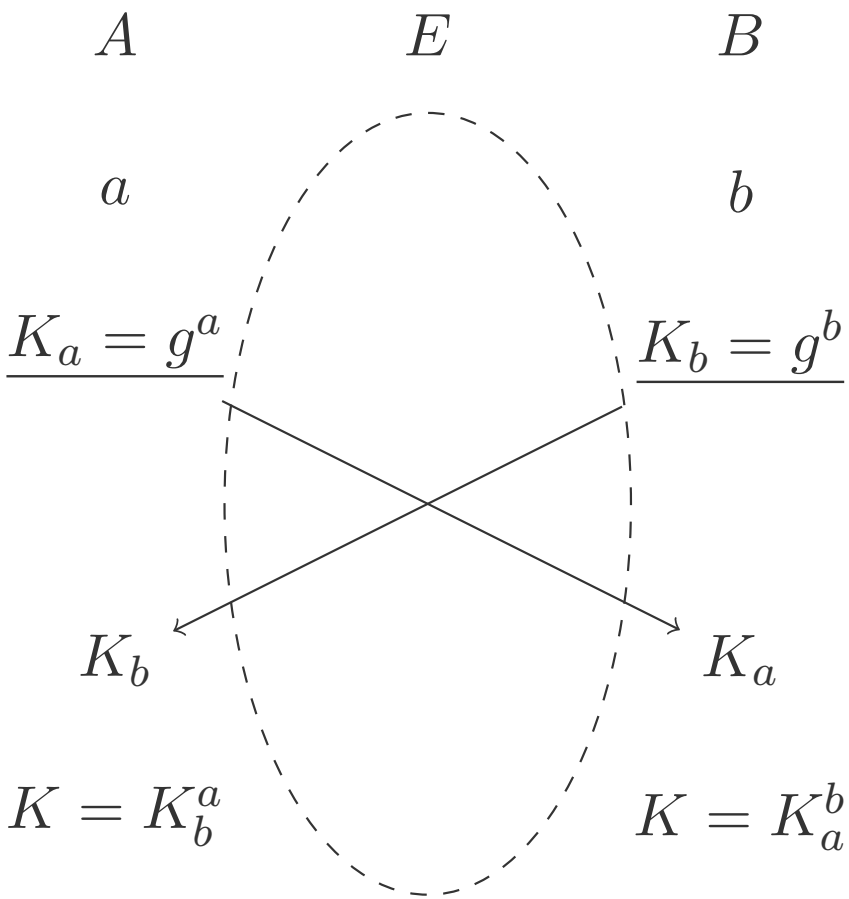
- Imamo jedan zajednički ključ K (poznat samo A-u i B-u)



- K se koristi i za enkripciju i za dekripciju

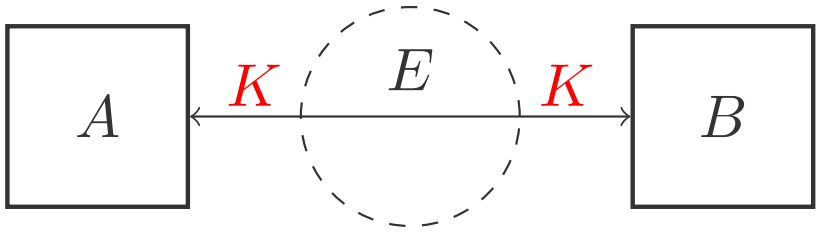
Diffie Hellman Key exchange

- Pretpostavimo da imamo generator g po prostom modulu n.



XOR Enkripcija

- Saljemo $M = m \oplus K$, gde je $\oplus$ bitovno ekskluzivno ili



$$m \xrightarrow{M = m \oplus K} m = M \oplus K$$

- Ako E sazna neko m_1, tada je svako drugo

$$m_i = M_i \oplus K = M_i \oplus M_1 \oplus m_1$$

- NE KORISTITI OVO!
- NI ono ranije

Simboli

- A, B - strane u konverzaciji
- S - server kome A i B *veruju*
- X, Y - idealizovane poruke
- $K, K_a, K_b, K_{ab}, K_{as}, K_{bs}$ - ključevi
- $\{X\}_K$ - predstavlja X enkriptovano sa K
- $\{X\}_K$ se dešifruje uz pomoć K^{-1} u slučaju da je K javni ključ, odnosno K ako je u pitanju simetrični ključ (očigledno iz konteksta)

$$\#(X)$$

- X je nova informacija
- Enkripcija nam ne garantuje da je neka šifra neprobojna, već nam samo daje *garanciju* da je niko neće probiti *uskoro*
- E bi mogao da koristi predefinisane napade

$$P \models X$$

- P veruje da važi X
- Centralna konstrukcija
- $P \models$ 'Q poseduje privatni ključ K^{-1}'
- $P \models$ 'Q je poslao poruku $\{X\}_K$'
- $P \models \#(N_a)$

$$P \mid\sim X$$

- P je poslao X nekada
- P je verovao da tada važi X
- $P \mid\sim$ 'Nedelja informatike je jedina nedelja'
- $P \mid\sim \{\text{Nedelja informatike je jedina nedelja}\}_K$
- $Q \models P \mid\sim X$

$$Q \lhd X$$

- Q je video X (potencijalno nakon dekripcije)
- Ovo dobijamo analizom protokola
- $Q \lhd$ 'Nedelja informatike je jedina nedelja'
- $Q \lhd \{\text{Nedelja informatike je jedina nedelja}\}_K$
- $Q \lhd \{X\}_K \not\Longrightarrow P \lhd X$
- Q ne vidi svoje poruke

$$P \overset{K}{\leftrightarrow} Q$$

- P i Q imaju zajednički ključ K
- P i Q mogu da koriste K za simetričnu kriptografiju
- Niko osim P, Q ne zna K
- $P \models P \overset{K}{\leftrightarrow} Q \implies Q \models P \overset{K}{\leftrightarrow} Q$

$$\overset{K}{\longmapsto} P$$

- P poseduje privatni ključ K^{-1}
- P je objavio javni ključ K
- Niko osim P ne zna K^{-1}
- $Q \models \overset{K}{\longmapsto} P \implies Q$ može da pošalje poruku $\{X\}_K$

$$S \mid\Rightarrow X$$

- S je autoritet da uradi X
- $P \mid\equiv S \mid\Rightarrow A \overset{K}{\leftrightarrow} B$
- $P \mid\equiv S \mid\Rightarrow \#(A \overset{K}{\leftrightarrow} B)$

Kvantifikatori

$$P \models S \models\!\Rightarrow A \overset{K}{\leftrightarrow} B$$

Ustvari znači

$$P \models S \models\!\Rightarrow \forall K.A \overset{K}{\leftrightarrow} B$$

Primetimo da sledeće formule imaju različito značenje

- $P \models S \models\!\Rightarrow \forall K.Q \models\!\Rightarrow A \overset{K}{\leftrightarrow} B$
- $P \models S \models\!\Rightarrow Q \models\!\Rightarrow \forall X.A \overset{K}{\leftrightarrow} B$

Stablo dokaza

- *Modus Ponens*

$$\frac{P \implies Q \qquad P}{Q}$$

- RSA

$$\dfrac{\dfrac{n = pq \qquad \phi = (p-1)(q-1)}{\phi = \varphi(n)} \qquad \dfrac{\dfrac{(e,\phi) = 1}{\exists x.ex \equiv_\phi 1}}{ed \equiv_\phi 1}}{\dfrac{\forall x.(x,n) = 1 \implies x^{ed} \equiv_n x \qquad (m,n) = 1}{m^{ed} \equiv_n 1}}$$

Enkripcija javnim ključem

$$\frac{P \models \overset{K}{\longmapsto} Q \qquad P \lhd \{X\}_{K^{-1}}}{P \models Q \mid\sim X}$$

P veruje da:

- Jedino Q zna K^{-1}
- P onda veruje da jedino Q može da enkriptuje X sa K^{-1}
- Primetimo da ovo ne znači da je Q poslao X direktno P-u

Enkripcija simetričnim ključem

$$\frac{P \mid\equiv P \overset{K}{\leftrightarrow} Q \qquad P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X}$$

P veruje da:

- Jedino P i Q
- P zna da on nije poslao $\{X\}_K$
- P onda veruje da je jedino Q može da enkriptuje X sa K

Nove poruke

$$\frac{P \models \#(X) \qquad P \models Q \mid\sim X}{P \models Q \models X}$$

- Ako je Q poslao X nedavno, onda X još uvek važi
- Ako ne bismo imali uslov da je X nastalo skoro, onda ne bismo imali garanciju da neko nije u međuvremenu probio X

$$X = P \overset{K}{\leftrightarrow} Q$$

Verovanje

$$\frac{P \models Q \models\!\!\Rightarrow X \qquad P \models Q \models X}{P \models X}$$

Delovi poruka

$$\frac{P \models X \qquad P \models Y}{P \models (X, Y)} \qquad \frac{P \models (X, Y)}{P \models X} \qquad \frac{P \models Q \models (X, Y)}{P \models Q \models X}$$

- Ako P veruje da X i Y, onda veruje da i $X \wedge Y$
- Ako P veruje da $X \wedge Y$, onda veruje da i X
- $(X, Y) = (Y, X)$

Delovi poruka

$$\frac{P \mid\equiv Q \mid\sim (X, Y)}{P \mid\equiv Q \mid\sim X}$$

Da li važi obrnuto?

$$\frac{P \mid\equiv Q \mid\sim X \qquad P \mid\equiv Q \mid\sim Y}{P \mid\equiv Q \mid\sim (X, Y)}$$

Ne, zato što bi to značilo da ih je Q poslao u isto vreme

Šta P vidi

- P vidi svaki deo poruke

$$\frac{P \lhd (X, Y)}{P \lhd X}$$

- P zna da dešifruje $\{X\}_K$ pod uslovom da zna simetrični ključ K

$$\frac{P \models P \overset{K}{\leftrightarrow} Q \qquad P \lhd \{X\}_K}{P \lhd X}$$

- P zna da dešifruje $\{X\}_K$ pod uslovom da zna privatni ključ K^{-1}

$$\frac{P \models \overset{K}{\longmapsto} P \qquad P \lhd \{X\}_K}{P \lhd X} \qquad \frac{P \models \overset{K}{\longmapsto} Q \qquad P \lhd \{X\}_{K^{-1}}}{P \lhd X}$$

Deo nove poruke

$$\frac{P \models \#(X)}{P \models \#(X, Y)}$$

- Ako je neki deo poruke nastao nedavno, onda je i cela poruka nastala nedavno

Simetričnost

$$\frac{P \models R \overset{K}{\leftrightarrow} T}{P \models T \overset{K}{\leftrightarrow} R} \qquad \frac{P \models Q \models R \overset{K}{\leftrightarrow} T}{P \models Q \models T \overset{K}{\leftrightarrow} R}$$

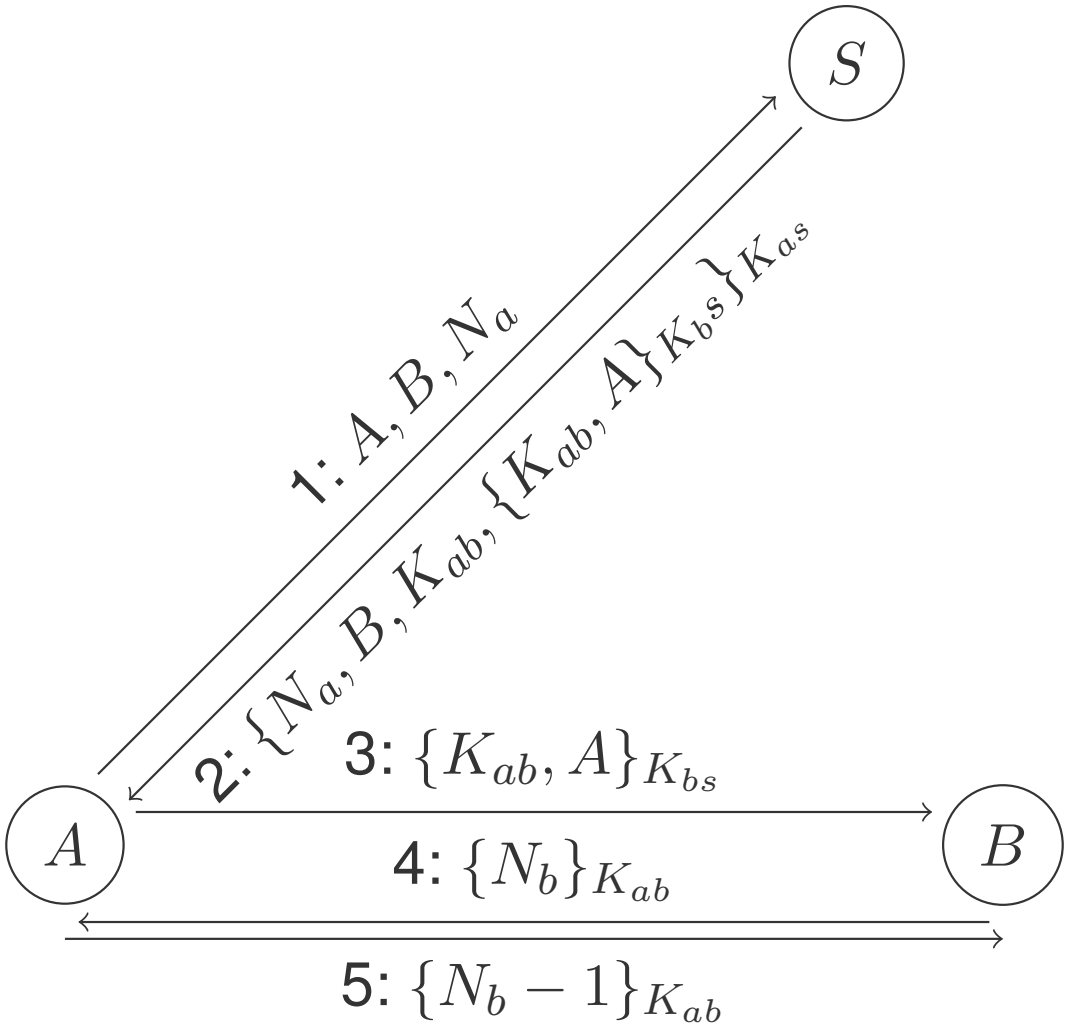
- Simetrični ključ je simetričan

Cilj

Mi želimo da A i B mogu da uspostave sigurnu komunikaciju

- $A \models A \overset{K}{\leftrightarrow} B \wedge B \models A \overset{K}{\leftrightarrow} B$
- $A \models B \models A \overset{K}{\leftrightarrow} B \wedge B \models A \models A \overset{K}{\leftrightarrow} B$
- ...
- ???
- $A \models\!\!\mid\!\overset{K}{\rightarrow} B$

Needham-Schroeder Protokol



Needham-Schroeder Protokol

Idealizovani protokol

$$P_1\ A \to S: \quad N_a$$

$$P_2\ S \to A: \quad \{N_a, A \overset{K_{ab}}{\longleftrightarrow} B, \#(A \overset{K_{ab}}{\longleftrightarrow} B), \{A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}\}_{K_{as}}$$

$$P_3\ A \to B: \quad \{A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}$$

$$P_4\ B \to A: \quad \{N_b, A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{ab}}$$

$$P_5\ A \to B: \quad \{N_b, A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{ab}}$$

Needham-Schroeder Protokol

Pretpostavke

- Postoje ključevi K_{as} i K_{bs} između, redom, A i S, kao i B i S

$$A \models A \overset{K_{as}}{\longleftrightarrow} S \quad S \models A \overset{K_{as}}{\longleftrightarrow} S$$

$$B \models B \overset{K_{bs}}{\longleftrightarrow} S \quad S \models B \overset{K_{bs}}{\longleftrightarrow} S$$

- S zna ključ koji će dodeliti A-u i B-u

$$S \models A \overset{K_{ab}}{\longleftrightarrow} B$$

Needham-Schroeder Protokol

Pretpostavke

- A i B veruju da će server napraviti novi ključ koji je dobar

$$A \models (S \models\!\!\Rightarrow A \overset{K}{\longleftrightarrow} B) \quad B \models (S \models\!\!\Rightarrow A \overset{K}{\longleftrightarrow} B)$$

$$A \models (S \models\!\!\Rightarrow \#(A \overset{K}{\longleftrightarrow} B))$$

- N_a, N_b i K_{ab} su nedavno generisani

$$A \models \#(N_a) \quad B \models \#(N_b)$$

$$S \models \#(A \overset{K_{ab}}{\longleftrightarrow} B) \quad \underline{B \models \#(A \overset{K_{ab}}{\longleftrightarrow} B)}$$

Needham-Schroeder Protokol

Analiza

- A prima poruku od S koju može da dešifruje

$$A \lhd \{N_a, (A \overset{K_{ab}}{\longleftrightarrow} B), \#(A \overset{K_{ab}}{\longleftrightarrow} B), \{A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}\}_{K_{as}}$$

- Kako $A \models \#(N_a)$

$$A \models S \models A \overset{K_{ab}}{\longleftrightarrow} B \quad A \models S \models \#(A \overset{K_{ab}}{\longleftrightarrow} B)$$

- Kako A veruje S-u

$$A \models A \overset{K_{ab}}{\longleftrightarrow} B \quad A \models \#(A \overset{K_{ab}}{\longleftrightarrow} B)$$

Needham-Schroeder Protokol

Analiza

- Kako $A \lhd \{A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}$

$$B \lhd \{A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}$$

- Kako $B \models B \overset{K_{bs}}{\longleftrightarrow} S$

$$B \models S \mid\sim A \overset{K_{ab}}{\longleftrightarrow} B$$

- Ako bismo imali $B \models S \models A \overset{K_{ab}}{\longleftrightarrow} B$ (imamo)

$$B \models A \overset{K_{ab}}{\longleftrightarrow} B$$

O čemu nismo pričali?

- Javnim ključevima
- Zajedničkim tajnama
- Hašovanju
- Protokolima koji nisu Needham-Schroeder

Hvala na pažnji