KERBEROS - NEEDHAM SCHRÖDER

ID NONCE

$\{|\ |\}_{pkB}$ → Asym encryption

1. $A \rightarrow B : \{|A, N_A|\}_{pkB}$
2. $B \rightarrow A : \{|N_A, N_B|\}_{pkA}$
3. $A \rightarrow B : \{|N_B|\}_{pkB}$

} Alice & Bob

$\Rightarrow$

NONCE value used once

$A \rightarrow \cdot \{|A, N_A|\}_{pk(B)} \quad \cdot \rightarrow B \{|x_A, x_{NA}|\}_{pk(B)}$

$A \leftarrow \cdot \{|N_A, x_{NB}|\}_{pk(A)} \quad \cdot \leftarrow B \{|x_{NA}, N_B|\}_{pk(x_A)}$

$A \rightarrow \cdot \{|x_{NB}|\}_{pk(B)} \quad \cdot \rightarrow B \{|N_B|\}_{pk(B)}$

1. $A \rightarrow B : \{|A, N_A|\}_{pk_B}$

2. $B \rightarrow A : \{|N_A, N_B|\}_{pk_A}$

$A \rightarrow B : \{|N_B|\}_{pk_B}$

A C B

$\{|A, N_A|\}_{pk(C)}$

$\{|A, N_A|\}_{pk(B)}$

и

$\{|N_A, N_B|\}_{pk(A)}$

$\{|N_B|\}_{pk(C)}$

$\{|N_B|\}_{pk(B)}$ →

1. $A \rightarrow B : \{|A, N_A|\}_{pkB}$
2. $B \rightarrow A : \{|N_A, N_B, B|\}_{pkA}$
3. $A \rightarrow B : \{|N_B|\}_{pkB}$

3. Messages & Deduction

$$\frac{\vdash A \qquad \vdash B}{\vdash A \wedge B}$$

$$\frac{enc(x, y) \qquad y}{x}$$

$$\frac{aenc(x, pk(y)) \qquad y}{x}$$

$\mathcal{X}$ - variables $x, y, z \ldots$

$\mathcal{N}$ - names $a, b, c \ldots$

$\mathcal{F}$ - functions $f, g, h \ldots$

$$t \in T(\mathcal{F}, \mathcal{X}, \mathcal{N})$$

$var(t) \rightarrow$ vars of t

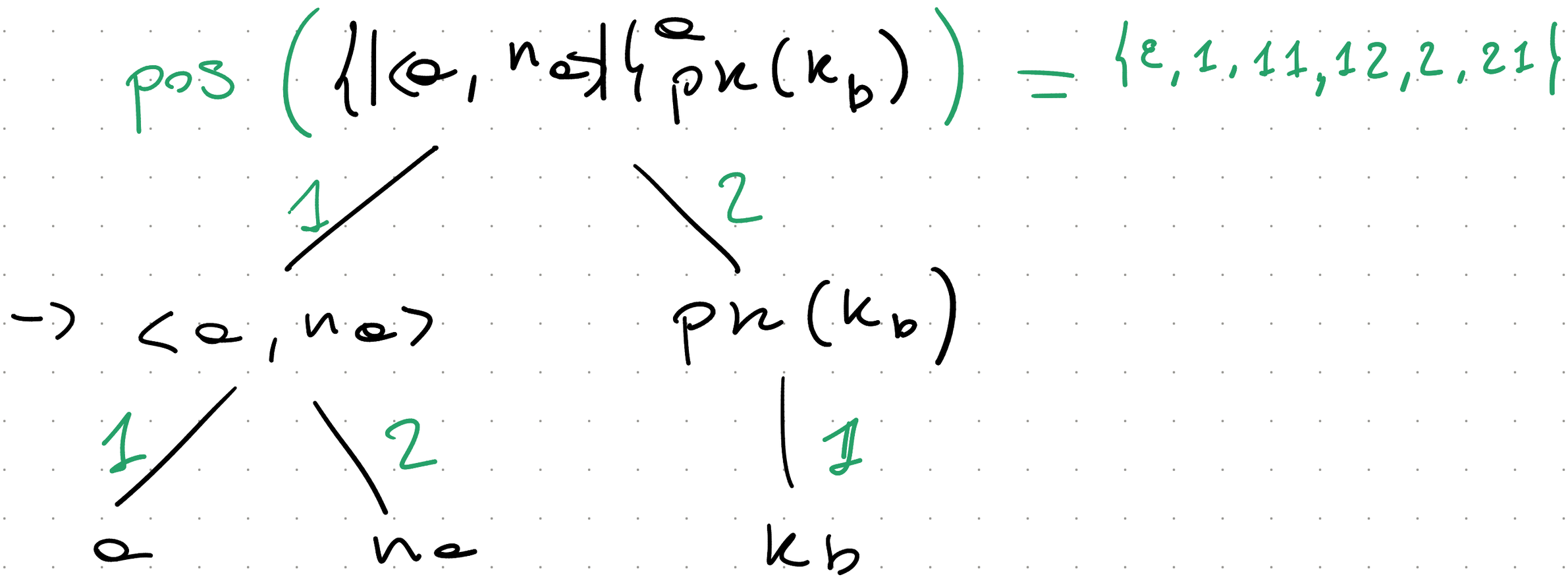
$n(t) \rightarrow$ names of t

$$vars(t) = \emptyset \equiv \text{"}t \text{ is ground"}$$

$$F_{std} = \{ senc, aenc, pair, pk \}$$

$$\{\!| A, N_A |\!\}_{pk_B} \rightsquigarrow aenc(pair(a, n_a), pk(k_b))$$

$$pos\left(\{\!|\langle a, n_a\rangle|\!\}_{pk(k_b)}\right) = \{\varepsilon, 1, 11, 12, 2, 21\}$$



$$pos(f(t_1 \dots t_n)) = \{\varepsilon\} \cup \bigcup_{i=1}^{n} i \cdot pos(t_i)$$

$$pos(x/n') = \{\varepsilon\}$$

$$\{|\langle a, n_a\rangle|\}_{pk(k_b)}|_1 = \langle a, n_a\rangle$$

$$u|_\varepsilon = u$$

$$u|_{1.2} = n_a$$

Substitution $\sigma : \mathcal{X} \to T(\mathcal{F}, \mathcal{X}, \mathcal{N})$

$\sigma(x) = x$ if $x \in Dom(\sigma)$

$\sigma(f(t_1 \ldots t_n)) = f(\sigma(t_1) \ldots \sigma(t_n))$

$u, v \in T(\ldots)$ are unifiable

if $\sigma(u) = \sigma(t)$ for some σ

$mgu(u, v) = \sigma$ is the most general unifier

most general means

if $\mu G = \nu G$ then $G = mgu(\mu, \nu) \cdot \theta$

3.2 Message Deduction

$$\frac{succ(m,k) \qquad k}{m}$$

Inference rule $\dfrac{u_1 \quad \cdots \quad u_n}{u}$

$$\mathcal{I}_{DY}: \left\{ \frac{x \quad y}{\langle x,y \rangle} \quad \frac{x \quad y}{\mathrm{Senc}(x,y)} \quad \frac{x \quad y}{\mathrm{Aenc}(x,y)} \quad \frac{\langle x,y \rangle}{x} \quad \frac{\langle x,y \rangle}{y} \quad \frac{\mathrm{Senc}(x,y) \quad y}{x} \quad \frac{\mathrm{Aenc}(x,\mathrm{pk}(y)) \quad y}{x} \right.$$

$$S_0 \overset{?}{\vdash} t$$

$$S_0 = \{\langle k_1, k_2 \rangle, \langle k_3, a \rangle, \{|n|\}^s_{\langle k_1, k_3 \rangle}\}$$

$$S_0 \overset{?}{\vdash} \langle n, a \rangle \quad \checkmark$$

$\checkmark$

$$S_0 = \{\langle k_1, k_2\rangle, \langle k_3, a\rangle, \{\!|\, n \,|\!\}^S_{\langle k_1, k_3\rangle}\}$$

$$\mathcal{I}_{DY}: \left\{ \frac{x \quad y}{\langle x,y\rangle} \quad \frac{x \quad y}{\mathrm{senc}(x,y)} \quad \frac{x \quad y}{\mathrm{aenc}(x,y)} \quad \frac{(x,y)}{x} \quad \frac{(x,y)}{y} \quad \frac{\mathrm{senc}(x,y) \quad y}{+} \quad \frac{\mathrm{aenc}(x,\mathrm{pk}(y)) \quad y}{x} \right.$$

$$\frac{\dfrac{\dfrac{}{\langle k_1, k_2\rangle}}{k_1} \quad \dfrac{\dfrac{}{\langle k_3, a\rangle}}{k_3}}{\dfrac{\{\!|\, n \,|\!\}_{\langle k_1, k_3\rangle} \quad \langle k_1, k_3\rangle}{n} \quad \dfrac{(k_3, a)}{a}}$$

$$\langle n, a\rangle$$

$S \vdash^{1}_{\mathcal{I}} t$ if $\dfrac{u_1 \quad \dots \quad u_n}{u}$, $t_1 \dots t_n \in S$, θ s.t. $t_i = u_i\theta$ and $t = u\theta$

$\dfrac{t_1 \quad \dots \quad t_n}{t}$ is an instance of

$S \vdash_{\mathcal{I}} t$ if there is a tree Π s.t.

- the leaves are in S
- all internal nodes are instances of rules in $\mathcal{I}$
- the root has label t.

Input: S, t

Output: yes/no $(S \overset{?}{\underset{\mathcal{I}}{\vdash}} t)$

1. let $S_0 = S$
2. let $S_{i+1} = S_i \cup \{u \mid S_i \vdash_{\mathcal{I}}^{1} u\} \cap st(S \cap \{t\})$
3. If $S_{i+1} = S_i$ then stop
4. Check wether $t \in S_i$

$\mathcal{I}$ is local if for any finite set S and t st. $S \vdash t$ there exist tree Π such that all labels in Π are subterms of $(S \cup \{t\})$