**NOTAÇÃO FORMAL PARA PROTOCOLOS CRIPTOGRÁFICOS**

Para facilitar a escrita na notação formal dos protocolos, seguem algumas explicações.

O que estamos usando é uma notação, porque só estamos preocupados com uma forma sintática (sintaxe), sem nos preocuparmos com a descrição formal da semântica das expressões da notação.

Assim, podem considerar para a lista de exercícios teóricos 2 e para as provas escritas, o seguinte:

<Etapa de Protocolo\_N> é uma linha na descrição de um protocolo, e pode ser vista, numa notação parecida com a BNF, que vocês já devem ter visto, na descrição de gramáticas na parte de Linguagens Formais.

<Etapa de Protocolo>, uma linha na descrição de um protocolo pode ser vista assim:

**<Emissor> 🡪 <Receptor> :** **<Ação do Protocolo>

 <Emissor> := <nome\_emissor>

 <Receptor> := <nome\_receptor>

<Ação do Protocolo> :=**  **<Ação1> || ... || <AçãoN>
 | [ <Ação1> || <Ação2> || .... || <AçãoN> ]**

onde o símbolo “**||**” é concatenação de mensagens e os símbolos “**[**“ e “**]**” são delimitadores de mensagens, quando necessário.

**<AçãoI> := E(K,M) ou EK(M) ou N<nome-emissor-nonce>**
 | **D(K,M)** ou **DK(M)** e **N<nome-emissor-nonce>**  onde N é um *nonce*, somente usado uma
 única vez numa comunicação.

Onde**: E = encripta**, **D = decripta**, **M = mensagem**,
 **K é uma chave (mestra-CT, sessão-S, pública-PU ou privada KR)**

**K := KU | KR | S** **| CT**

(ou seja, **K** é uma chave que pode ser pública, privada ou de sessão ou até uma chave que só existe entre um provedor de chaves e uma entidade de protocolo – como Alice, Bob, Trent, .... – ou uma chave-mestra **CT** como aparece numa comunicação entre um terminal bancário e um banco.

**KUA** ou **PUA** = chave pública, onde A é uma entidade de protocolo que envia ou recebe mensagens.
 **KRA** ou **PRA** = chave privada, onde A é uma entidade de protocolo que envia ou recebe mensagens.

**KS** ou **KS** = chave de sessão (de duração da sessão)
**CT** = chave mestra (de longa duração)

Se precisarem assinar uma mensagem com uma chave **K**, use **SK(M)**,onde **K** pode ser qualquer dos casos acima.

Se precisar verificar a assinatura com uma chave **K**, use **VK(M)**.

Se precisarem representar uma função Hash de uma mensagem M, isto pode ser escrito assim: **H(M)**

Se precisarem representar um MAC com Hash, uma MAC onde se usa uma função Hash, podem escrever: **HMAC(K,M)**, porque existe uma concatenação de uma chave com uma mensagem.

Se precisarem descrever uma senha: **senha(A)** , onde **A** é uma entidade de protocolo que envia ou recebe mensagens.

Uma chave de criptografia de chave (**KEK**) pode ser: **KEKA** , onde **A** é uma entidade de protocolo que envia ou recebe mensagens. Uma **KEK** é construída a partir de um Hash de uma senha e um salt: **H(senha, salt)**. Esta parte, criptografia baseada em senha, não foi explicada.

**Qualquer notação necessária, vislumbrada por vocês e que não esteja aqui, pode ser usada, mas apenas deve ser indicada o que significa de maneira informal.**