e, ao mesmo tempo, impedir o ataque acima, o usuário datilografa n no terminal e r é então calculado como sendo

$$r := CS(n). \qquad (1)$$

Agora, o ataque acima não tem mais sucesso, pois dado n, obtém-se apenas CS(r) = CS(CS(n)): o acesso a r é impedido.

Analogamente ao que acontece no protocolo anterior, chaves precisam ser protegidas no sistema central. Lá CA necessitava de proteção, aqui CT necessita de proteção. Cuidaremos desse problema mais adiante.

6. *Exercícios*

1. No protocolo da sessão 3 (figura 1), se r for eliminado das mensagens o oponente pode gravar uma sessão de A e, mais tarde, numa segunda sessão, fazer-se passar pelo sistema perante A.

2. No mesmo protocolo da figura 1, se r' for eliminado das mensagens o oponente pode gravar uma sessão de A e mais tarde fazer-se passar por A perante o sistema.

3. Altere o protocolo da figura 1, dando uma implementação para sistemas de chave pública.

4. Implemente um mecanismo de autenticação de dados invariantes com o tempo baseado num sistema de chave pública. Nesse caso é ainda necessário um dispositivo criptográfico inviolável?