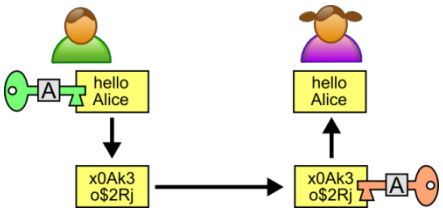
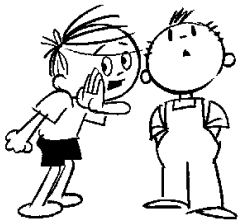
Problema 1: Segurança na NET - Resolução





Pois é assim:

A Alice mete o segredo na mala, fecha-a com o seu aloquete e envia ao Bob.

O transportador não pode ler a mensagem porque não tem a chave; mas o Bob também não.

Então o Bob volta a fechá-la com o seu aloquete e reenvia para a Alice.

A mala viaja de volta fechada com dois aloquetes.

Agora a Alice abre o seu aloquete e reenvia ao Bob.

Ao recebê-la Bob sabe que vem da Alice.

Abre o seu aloquete e lê a mensagem.

Se foi esta a solução que encontrou descobriu o algoritmo de Diffe-Helman uma analogia do algoritmo matemático que se usa nas comunicações seguras na NET.

Supondo que a Alice quer transmitir um número g esse algoritmo funciona assim:

i) Alice e Bob acordam, na rede insegura, num primo p muito grande;
ii) Alice escolhe uma chave a e transmite $g^a \bmod p$;
iii) Bob escolhe uma chave b e volta a fechar $g^a \bmod p$ calculando $g^{ab} \bmod p$ que reenvia para a Alice;

iv) Alice abre o seu aloquete extraindo a raiz de índice a a g^{ab} e envia $g^b \bmod p$ para Bob;

v) Bob extrai a raiz de índice b a g^b para abrir a mensagem.

Admite-se, mas não está provado, que o algoritmo é seguro. Está contudo provado que os algarismos mais significativos da mensagem que circula na Net se distribuem uniformemente pelo são vistos como ruído por um potencial interceptor.