4.4 Secret Communication without Key Exchange

Even without exchanging keys in advance a confidential conversation is possible. (Note that this protocol also is not secure from the man in the middle.)

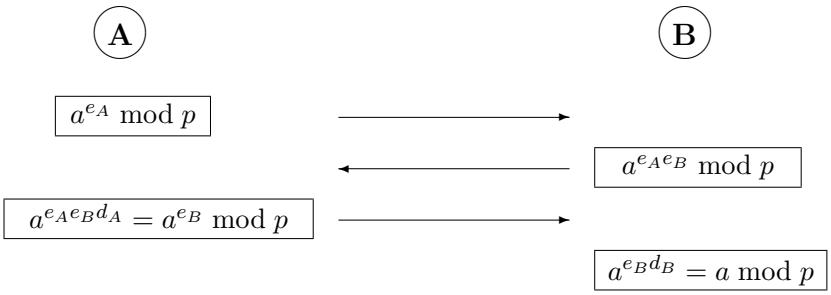
An analogy from veryday life illustrates the idea:

- Alice puts her message in a box and locks it with a padlock whose key is hers and not available to anyone else.
- Of course Bob is unable to open the box. Instead he locks it with another padlock of his own. He returns the doubly locked box to Alice.
- Alice removes her padlock and returns the box that is locked with Bob's padlock only.
- Bob removes his padlock, opens the box, and reads the message.

This cryptographic protocol is called the Massey-Omura scheme or Shamir's no-key algorithm. It may be implemented with the discrete exponential function. Its security relies on the discrete logarithm assumption:

The procedure uses a public large prime number p. Alice and Bob each choose a pair of exponents d and e with $ed \equiv 1 \pmod{p-1}$, hence $a^{de} \equiv a \pmod{p}$ for all integers $a \in \mathbb{Z}$. Each one keeps *both* of their exponents secret.

Then Alice sends a message a to Bob according to the following protocol:



An attacker who is able to compute discrete logarithms is also able to compute the exponent e_B from the intercepted ciphertexts $a^{e_A} \bmod p$ and $a^{e_A e_B} \bmod p$. From this she computes d_B by congruence division and solves for a.

This is the only known attack. Hence the protocol is secure from Eve as long as the discrete logarithm assumption holds. To be secure from Mallory the protocol must be supplemented by an authentication phase.