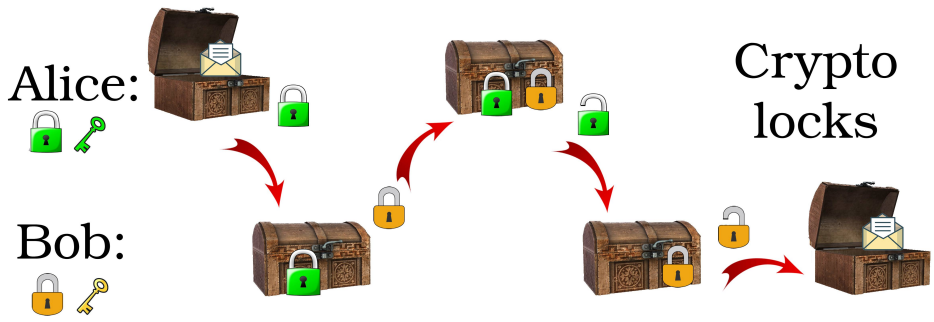
Problem 9. «Crypto locks»

Alice and Bob are wondering about the creation of a new version for the Shamir three-pass protocol. They have several ideas about it.

The Shamir three-pass protocol was developed more than 40 years ago. Recall it. Let p be a big prime number. Let Alice take two secret numbers c_A and d_A such that $c_A d_A = 1 \bmod (p-1)$. Bob takes numbers c_B and d_B with the same property. If Alice wants to send a secret message m to Bob, where m is an integer number $1 < m < p-1$, then she calculates $x_1 = m^{c_A} \bmod p$ and sends it to Bob. Then Bob computes $x_2 = x_1^{c_B} \bmod p$ and forwards it back to Alice. On the third step, Alice founds $x_3 = x_2^{d_A} \bmod p$ and sends it to Bob. Finally, Bob recovers m as $x_3^{d_B} \bmod p$ according to Fermat's Little theorem.

It is possible to think about action of c_A and d_A over the message as about locking and unlocking, see the picture below.



Alice and Bob decided to change the scheme by using symmetric encryption and decryption procedures instead of locking and unlocking with c_A, c_B, d_A and d_B.

Q1 Propose some simple symmetric ciphers that would be possible to use in such scheme. What properties for them are required? Should Alice and Bob use the same cipher (with different own keys) or not?

Q2 **Problem for a special prize!** Could you find such symmetric ciphers that make the modified scheme to be secure as before? Please, give your reasons and proofs.