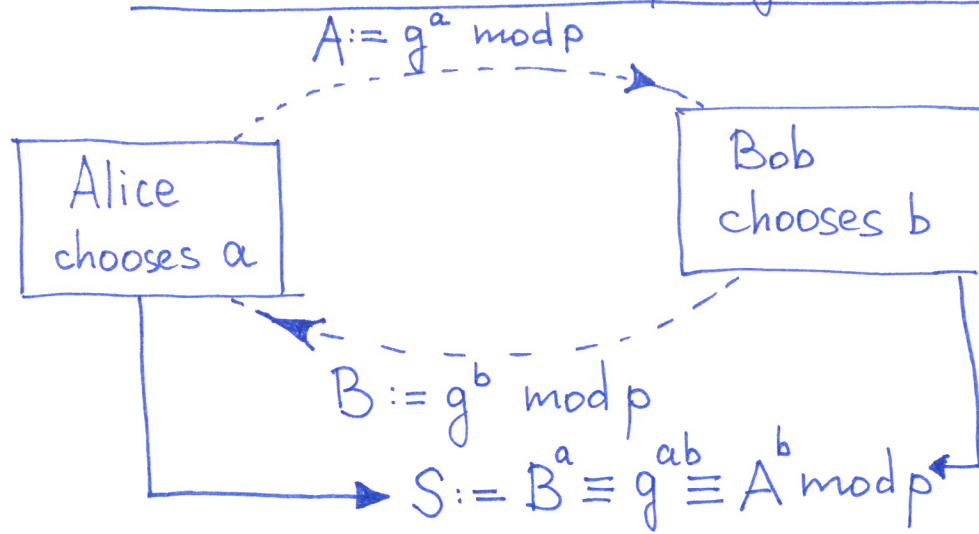
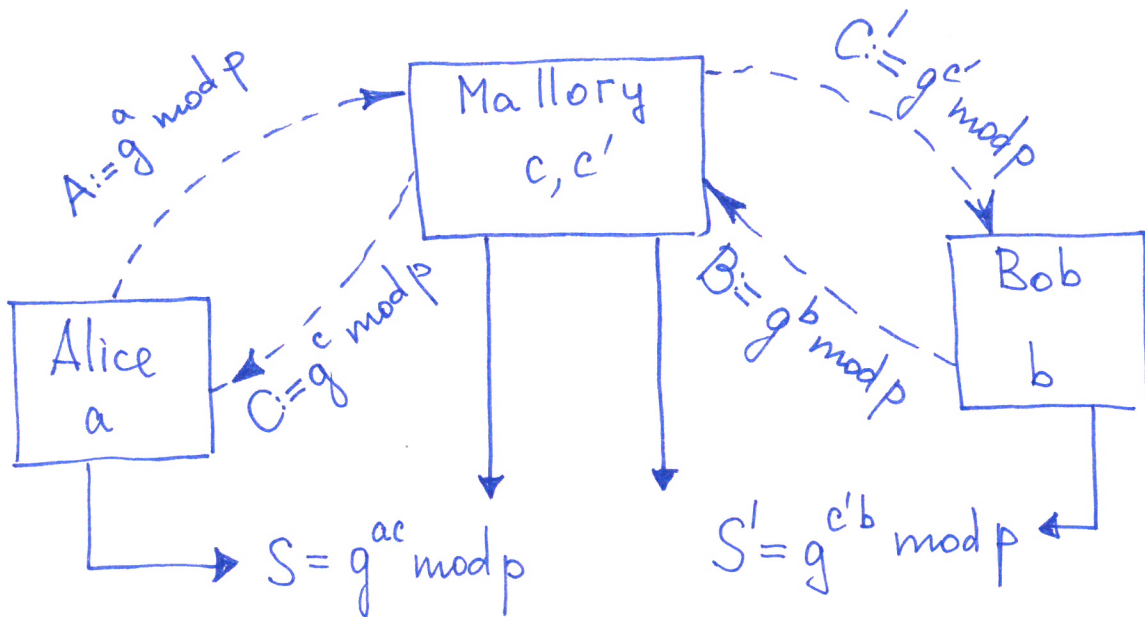


Diffie - Hellman key agreement

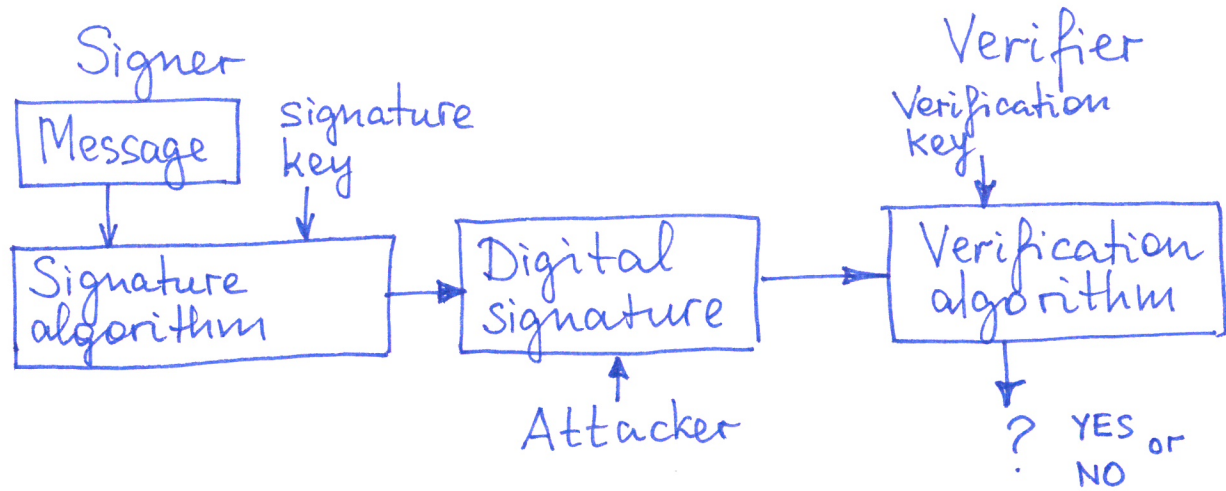


Active attack by Mallory

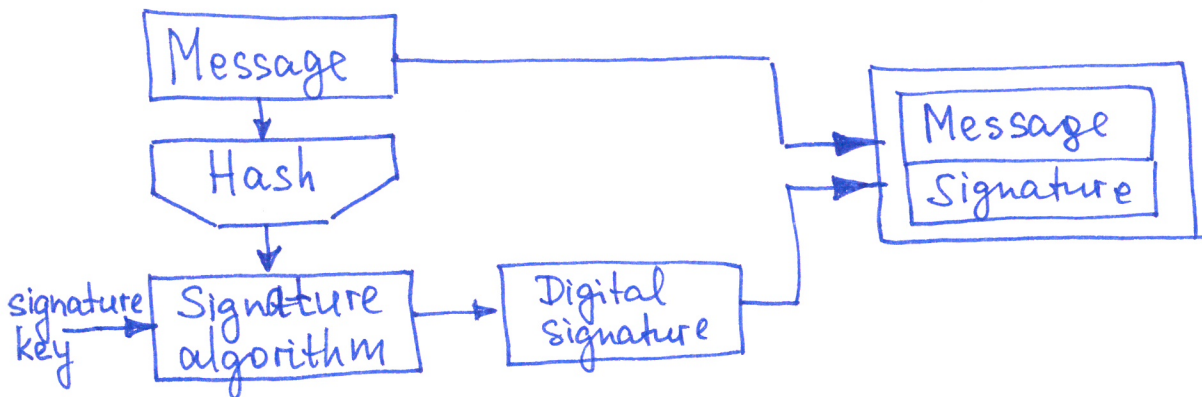


Mallory = (wo)man-in-the middle attack

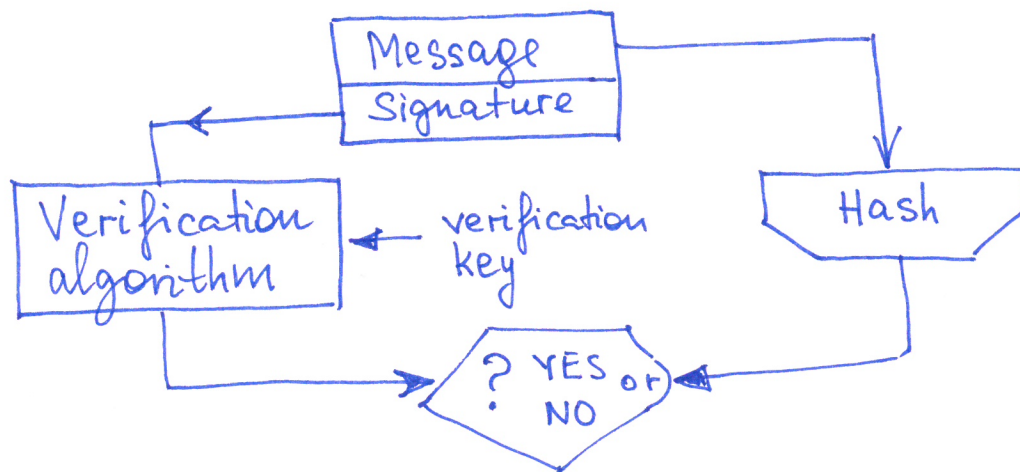
Basic model of DSS



DSS with appendix: signing



DSS with appendix: verifying



Reasons for hashing: efficiency, preventing the existential forgery, preventing modification attacks

Disadvantages of the DSS with appendix: requires hashing, both message and signature should be sent to the verifier.