- 1. Alice sends a cryptogram $m^e \mod n$ to Bob. Can adversary Carol recover m if $m^e < n$?
- 2. Alice sends the same RSA encrypted message to three different people with public keys n=87, n=115, n=187. Let the public exponent be 3. Adversary Carol intercepts 3 cryptograms $c_1=43, c_2=80, c_3=65$. Assume that the cryptograms were sent in order. It means that cryptogram 43 was sent to a recipient with modulus 87, cryptogram 80 was sent to a recipient with modulus 115, etc. Can Eve recover the message without factoring public keys?
- 3. Adversary Carol intercepted two RSA cryptograms, $y_1 = 537$ sent by Alice to Bob, and $y_2 = 285$ sent by Alice to Eve. Alice knows that Bob's public exponent $e_1 = 18$, and public modulus $n_1 = 943$, while Eve's public exponent $e_2 = 19$, and her public modulus $n_2 = 943$. What is the message m sent by Alice to Bob and Eve?