HW2 – Extra credit problems

Yi Xue 04/10/2016

Extra credit problem from Stallings:

9-7. Answers : not safe to generate new keys from old modulus.

Given N, e and d, there is some published algorithm to do factorial attack on RSA algorithms.

http://www.di-mgt.com.au/rsa_factorize_n.html
reference:

Boneh, D. *Twenty Years of Attacks on the RSA Cryptosystem*, Notices of the American Mathematical Society, 46(2):203-213, 1999

9-15. Answers:

BG sends to B the block : [BG, E(PUb, M), B]
“E(PUb, M]” is the message A previously sent to B.

B replies to BG : [B, E(PUbg, M), BG]
When BG receives the message, he can decrypt the message with his private key.