

Mã hoá với Textbook RSA

Bài tập 1: Alice đưa cho Bob khoá công khai RSA của cô ấy: modulus $N = 2038667$ và số mũ $e = 103$.

1. Bob muốn gửi cho Alice thông điệp $m = 892383$. Bản mã mà Bob gửi cho Alice là gì?
2. Alice biết rằng modulus N của cô ấy là tích của hai số nguyên tố, một trong hai số là $p = 1301$. Hãy tìm số mũ giải mã d cho Alice.
3. Alice nhận được bản mã $c = 317730$ từ Bob. Hãy giải mã.

Bài tập 2: Khoá công khai RSA của Bob có modulus $N = 12191$ và số mũ $e = 37$. Alice gửi cho Bob bản mã $c = 587$. Không may, Bob đã chọn modulus kích thước quá nhỏ. Bạn hãy giúp Oscar giải mã bằng cách phân tích thừa số nguyên tố của N và giải mã thông điệp của Alice. (Gợi ý: N có một thừa số nguyên tố nhỏ hơn 100.)