1082 作業五

繳交日期 109/05/08(五) 13:10

1. Suppose Alice uses the RSA method as follows. She starts with a message consisting of several letters, and assigns $a = 1$, $b = 2$, ..., $z = 26$. She then encrypts each letter separately. For example, if her message is "cat", she calculates $3^e \pmod{n}$, $1^e \pmod{n}$, and $20^e \pmod{n}$. Then she sends the encrypted messages to Bob. Explain how Eve can find the message without factoring n. In particular, suppose $n = 11771$ and $e = 17$. Eve intercepts the message

   1387 3011 1387 2244 4658 7799

   Find the message without factoring 11771 (because n is not too large, you might want to write a simple C/C++/python/matlab program to help yourself calculating the result)

2. Naïve Nelson uses RSA to receive a single ciphertext c, corresponding to the message m. His public modulus is n and his public encryption exponent is e. Since he feels guilty that his system was used only once, he agrees to decrypt any ciphertext that someone sends him, as long as it is not c, and return the answer to that person. Evil Eve sends him the ciphertext $2^e c \pmod{n}$. Show how this allows Eve to find m.

3. Let p be a large prime. Alice wants to send a message m to Bob, where $1 \le m \le p-1$. Alice and Bob choose integers a and b relatively prime to $p-1$. Alice computes $c \equiv m^a \pmod{p}$ and sends c to Bob. Bob computes $d \equiv c^b \pmod{p}$ and sends d back to Alice. Since Alice knows a, she finds a_1 such that $aa_1 \equiv 1 \pmod{p-1}$. Then she computes $e \equiv d^{a_1} \pmod{p}$ and sends e to Bob. Explain what Bob must now do to obtain m.