RSA Cryptography

Alice wants to receive a secure one-word message from Bob

- Alice Chooses prime numbers p,q whose product is greater than 26.
- (in practice, these would be very large numbers, and their product would be huge.)
- Ann computes n=pq
- Alice chooses a positive integer e that is relatively prime to (p-1)(q-1)
- Alice computes the an integer d that is a positive multiplicative inverse of e, mod (p-1)(q-1)
- The numbers n,e are called the Public Key. Alice sends Bob the n and the e, the Public Key. (Alice does not send Bob the values of p,q,d.)

Bob has a word consisting consisting of k letters chosen from the set {a,b,…,z}. The letters are denoted $\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_k$ (The word would be written with the letters side-by-side with no commas, $\mathcal{L}_1\mathcal{L}_2 \dots \mathcal{L}_k$)

- Bob receives the Public Key n, e from Alice.
- Bob repeats the following steps for each letter $\mathcal{L}_j$ in his word, for $j = 1,2, \dots k$
    - He converts the letter $\mathcal{L}_j$ to a number in the range 1 – 26, called M_j
    - Then he computes $(M_j)^e$ mod n. The result is denoted C_j. So
    $$C_j = (M_j)^e \bmod n$$
- Bob sends Alice the list of numbers $C_1, C_2, \dots, C_k$

Alice

- Alice receives the list of numbers $C_1, C_2, \dots, C_k$ from Bob
- Alice repeats the following steps for each number C_j in the list, for $j = 1,2, \dots k$
    - She computes $(C_j)^d$ mod n. The result is M_j.That is,
    $$M_j = (C_j)^d \bmod n$$
    - She converts converts the number M_j to letter $\mathcal{L}_j$
- The result is a list of letters $\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_k$
- The resulting word is $\mathcal{L}_1\mathcal{L}_2 \dots \mathcal{L}_k$

Observations:

- Alice does not send p,q,or d. She only sends Bob n and e.
- Without knowing the value of d, one cannot decrypt Bob's message.
- And without knowing the values of p, q, one cannot find d.
- One could guess values of p,q by factoring n. But in practice, n is a very large number, and so factoring n is not feasable in a reasonable time scale.