Cryptology Packet Ch 5.3

ID: 1747

April 2023

1. Suppose that you are listening in on Bob's public transmission and you hear that $pq = 21$ and $E = 5$. Recover $(p-1)(q-1)$ and D

   pq=21 so $p = 7, q = 3$ and $(p-1)(q-1) = 12$
   $D \equiv E^{-1} \mod (p-1)(q-1)$
   $D \equiv 5^{-1} \mod 12$
   $D * 5 \equiv 1 \mod 12$
   $D = 5$

2. You are a secret agent. An evil spy with shallow number theory skills uses the RSA Public Key Coding System in which the public modulus is $n = 1537$, and the encoding exponent is $E = 47$. You intercept one of the encoded secret messages being sent to the evil spy, namely the number 570. Using your superior number theory skills, decode this message, thereby saving countless people from the fiendish plot of the evil spy.

   $pq = 1537$
   $M^{ED} \equiv M \mod pq$
   Have M, E, pq. Need to find $(p-1)(q-1)$ using $M^{(p-1)(q-1)} \equiv 1 \mod pq$ and D using $D \equiv E^{-1} \mod (p-1)(q-1)$

   $M^{(p-1)(q-1)} \equiv 1 \mod pq$
   $570^{(p-1)(q-1)} \equiv 1 \mod 1537$
   $570^{1456} \equiv 1 \mod 1537$
   $pq = 1537$ so $p = 29, q = 53$ and $(p-1)(q-1) = 1456$

   $D \equiv E^{-1} \mod (p-1)(q-1)$
   $D \equiv 47^{-1} \mod 1456$
   $D * 47 \equiv 1 \mod 1456$
   $D = 31$

   To check:
   $M^{ED} \equiv M \mod pq$
   $570^{47*31} \equiv 570 \mod 1537$
   $570^{1457} \equiv 570 \mod 1537$

3. Summarize RSA encryption and the advantages it offers in your own words.

   RSA Encryption, also called Public Key Cryptography or asymmetric cryptography, is a way to communicate a message securely even when a secret key has not been designed ahead of time. By generating a public-private key combination, any two users can pass a message securely by simply sharing their public key.

   The steps involved in RSA encryption system are:

   (a) Generating a public and private key

   (b) Encrypting by using the public key

   (c) Decrypting using the private key

   Even if everyone knows the public key, the message cannot be decrypted without knowing the private key. To generate this combination, a user, let's say Alice will choose two prime numbers, a public exponent E and a private exponent D which are multiplicative modulo inverses of each other. Once these parameters are set, another user, Bob can send a message to Alice by using her public exponent. Alice can use her private key or exponent to decode the message. The biggest advantage of RSA encryption is of course the security of encryption that it gives. By using large prime numbers, RSA algorithm becomes difficult for others to crack. Because of this, it is used in industries that need secure transactions like online banking, e-commerce and for digital signature.

4. Can you see any weaknesses in RSA? There are a couple and one has to make a few simple modifications to the messages being sent and the algorithm to avoid them. For the sake of simplicity, the method discussed here is the simplest version and in practice more sophisticated methods (based on the same idea) are used.

   If small exponents are used for encryption, then M^E is less than $\mod pq$ and can be decrypted by taking the the root of the cipher text. Also, p and q need to be unique. If they are used again, they can be factored using the GCD algorithm. This requires a good random number generator.

   Some methods by which RSAs have been broken include Chinese Remainder Theorem and Coopersmith's attack. To avoid these problems, padding is added to the RSA cryptosystem. Padding is the addition of random bytes so the original message length cannot be deciphered. Also, the same message that is encrypted multiple times will appear different because of the padding. This randomized padding can prevent guessing and breach of similar looking encrypted messages.

Another disadvantage of the RSA is that strong encryption with RSA requires large prime numbers but this increases the size of the encryption key and can lead to slow processing time compared to other algorithms.