RSA Algorithm

DR. VASUDHA ARORA

VASUDHA.ARORA@GDGU.ORG, VASUDHARORA6@GMAIL.COM

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GD GOENKA UNIVERSITY, GURUGRAM

RSA Algorithm

- The most important public-key cryptosystem is the RSA cryptosystem on which one can also illustrate a variety of important ideas of modern public-key cryptography.
- Invented in 1978 by Rivest, Shamir, Adleman
- Basic idea: prime multiplication is very easy, integer factorization seems to be unfeasible.
- RSA Algorithm is based on mathematical fact that is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product.
- The private and public keys in RSA are based on very large prime numbers.
- The real challenge in case of RSA is the selection and generation of the public and private keys.
- The algorithm is very simple and easy to understand
- best known & widely used public-key scheme

RSA Algorithm-Steps

1. Choose two large prime numbers P and Q
2. Calculate N = P x Q
3. Select the public key (i.e. Encryption Key), say E, such that it is not a factor of (p-1) and (Q-1)

   $\varnothing(N)=(P-1)(Q-1)$ where $1<E<\varnothing(N)$, $\gcd(e,\varnothing(N))=1$
4. Select the private key (i.e. Decryption key), say D, such that the following equation is true:

   (D x E) mod (p-1) x (Q-1) = 1 , and $0\leq D\leq N$
5. publish their public encryption key: PU={E, N}
6. keep secret private decryption key: PR={D, N}

RSA Algorithm-Example

- Let P = 7 and Q = 17
- N = P x Q = 7 x 17 = 119
- (P-1) x (Q-1) = 6 x 16 = 96
- Factors of 96 are 2,2,2,2,2 and 3, therefore our public key should not have a factor of 2 and 3.
- Let's choose the key value of E as 5.
- Select the private key D such that (D x E) mod (p-1) x (Q-1) = 1, Let us choose D as 77 as

  (5 x 77) mod 96 = 385 mod 96 = 1, which satisfies our condition

RSA Encryption & Decryption

1. For encryption, calculate the ciphertext C from the plaintext P as follows:

   $C = P^E \bmod N$

2. Send the C as ciphertext to the receiver.

3. For decryption, calculate the plain text from the ciphertext as follows:

   $P = C^D \bmod N$

RSA Algorithm-Example

Encryption Decryption using RSA:

- Let us assume that we want to encrypt a single alphabet F using this scheme
- A is the sender and B is the receiver of the message.
- A encrypts the message that is, F , using B's public key (5) generated by RSA algorithm.
- For Alphabets , we use a numeric scheme to convert an alphabet into a number such as A replaced by 1, B by 2 and so on.
- As per this rule we would be having f as 6 and hence F is encoded to 6 initially.
- We calculate ciphertext C as $C = P^E \bmod N$
- hence, here $C = 6^5 \bmod 119$

RSA Algorithm-Example

- which comes out to be 41.
- This encrypted information is sent over the network to the receiver B.
- At Receiver's End:

5. calculate the plain text from the ciphertext as follows:

   $P = C^D \bmod N$

- $P = 41^{77} \bmod 119$
- which comes out to be 6
- it is then decoded back to F to get the original plaintext back.

Private-key versus public-key cryptography

- The prime advantage of public-key cryptography is increased security - the private keys do not ever need to be transmitted or revealed to anyone.
- Public key cryptography is not meant to replace secret-key cryptography, but rather to supplement it, to make it more secure.
- Example RSA and DES are usually combined as follows
  1. The message is encrypted with a random DES key
  2. DES-key is encrypted with RSA
  3. DES-encrypted message and RSA-encrypted DES-key are sent.

This protocol is called RSA digital envelope.

- In software (hardware) DES is generally about 100 (1000) times faster than RSA.

If *n* users communicate with secrete-key cryptography, they need $n(n-1)/2$ keys. In the case they use public key cryptography $2n$ keys are sufficient.

Public-key cryptography allows spontaneous communication.

Private-key versus public-key cryptography

- If RSA is used for digital signature then the public key is usually much smaller than private key => verification is faster.

• An RSA signature is superior to a handwritten signature because it attests both to the contents of the message as well as to the identity of the signer.

As long as a secure hash function is used there is no way to take someone's signature from one document and attach it to another, or to after the signed message in any way.

The slightest change in a signed message will cause the digital signature verification process to fail.

• Digital signature are the exact tool necessary to convert even the most important paper based documents to digital form and to have them only in the digital form.