

Encryption RSA

Dr. Talal Alkharobi

2

RSA algorithm

- Invented in 1978 by Rivest, Shamir, and Adleman.
- Procedure
 - Find P and Q , two large (e.g., 1024-bit) prime numbers.
 - Choose E such that
 - $1 < E < P*Q$
 - E and $(P-1)*(Q-1)$ are *relatively prime* (they have no prime factors in common)
 - E does not have to be prime, but it must be odd

3



RSA algorithm

- Compute D (*multiplicative inverse of E*) such that
 - $(D * E - 1)$ is evenly divisible by $(P-1)(Q-1)$.
 - $D * E = 1 \pmod{(P-1)(Q-1)}$, and they call D the

$$D = \frac{X * (P - 1)(Q - 1) - 1}{E}$$

- Find an integer X which causes the above result D to be an integer,

4



RSA algorithm encryption

- The function is $C = T^E \pmod{P * Q}$, where
 - C is the ciphertext (a positive integer),
 - T is the plaintext (a positive integer),
 - T , must be less than the modulus, PQ .
 - E and $P * Q$ are the public key



RSA algorithm decryption

5

- The function is $T = C^D \bmod P*Q$, where
 - T is the reconstructed plaintext (a positive integer),
 - C is the received ciphertext (a positive integer),
 - D is the private Key



RSA algorithm

6

- You can publish your public key freely, because there are no known easy methods of calculating D , P , or Q given only (PQ, E) (the public key).
- If P and Q are each 1024 bits long, how much does it need to factor $P*Q$ to find them??

7



Number of prime numbers

- Even though the total number of primes is infinite, one could still ask "Approximately how many primes are there below 100,000?", or "How likely is a random 20-digit number to be prime?".
- The prime counting function $\pi(x)$ is defined as the number of primes up to x . There are known algorithms to compute exact values of $\pi(x)$ faster than it to compute each prime up to x .
- $\pi(100000) = 9592$, $\pi(10^{20}) = 2,220,819,602,560,918,840$.
- For larger values of x , beyond the reach of modern equipment, the prime number theorem provides a good estimate: $\pi(x)$ is $x/\ln(x)$.

$$\pi(2^{1024}) \approx \frac{2^{1024}}{\ln(2^{1024})} = \frac{2^{1024}}{1024 \ln(2)} \approx \frac{2^{1024}}{2^{10}} = 2^{1014}$$


8



Example

- $P = 61$
- $Q = 53$
- $P*Q = 3233$
- $E = 17$
- $D = ?$

$$D = \frac{X * (P - 1)(Q - 1) - 1}{E}$$




Example

$$D = \frac{X * (P-1)(Q-1) - 1}{E}$$

- D = 2753

X	X(P-1)(Q-1)+1	D
1	3121	183.5882
2	6241	367.1176
3	9361	550.6471
4	12481	734.1765
5	15601	917.7059
6	18721	1101.235
7	21841	1284.765
8	24961	1468.294
9	28081	1651.824
10	31201	1835.353
11	34321	2018.882
12	37441	2202.412
13	40561	2385.941
14	43681	2569.471
15	46801	2753
16	49921	2936.529
17	53041	3120.059
18	56161	3303.588
19	59281	3487.118
20	62401	3670.647

10



Encryption

- To encrypt the plaintext value 123
- $(123^{17}) \bmod 3233 =$
- $(337587917446653715596592958817679803) \bmod 3233 =$
- 855

