CS 70 Discrete Mathematics and Probability Theory
Summer 2020 Course Notes

DIS 3B

1 RSA Warm-Up

Consider an RSA scheme with modulus $N = pq$, where p and q are distinct prime numbers larger than 3.

(a) What is wrong with using the exponent $e = 2$ in an RSA public key?

$p-1$ $q-1$ even!

2^{-1} does not exist!

(b) Recall that e must be relatively prime to $p-1$ and $q-1$. Find a condition on p and q such that $e = 3$ is a valid exponent.

$p-1, q-1$

$3k$ 3ℓ

~~$p = 3k+1$~~ $p = 3k+2$

~~$q = 3\ell+1$~~ $q = 3\ell+2$

(c) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

$(85, 3)$

N e

pq

(d) What is the private key?

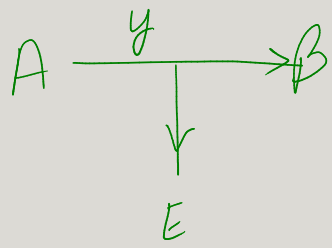
$3^{-1} \bmod 64$

$\equiv 43 \equiv -21$

(e) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message $E(x)$ she sends using the public key?

$10^3 \bmod 85$ $1000 \bmod 85$

$100 \cdot 10 \equiv 15 \cdot 10 \equiv \boxed{65} \bmod 85$



Public: (N, e) — product of 2 primes p, q; e has mult inv mod (p-1)(q-1)

$y \equiv x^e \bmod N$

$y^d \equiv x^{ed} \equiv x \bmod N$

ALGO

Private

Bob's d

$d \equiv e^{-1} \bmod (p-1)(q-1)$

FLT

$x^{p-1} \equiv 1 \bmod p$

$x^{p-1} - 1 \equiv 0 \bmod p$

q

$x^{k(p-1)(q-1)} \bmod p \Rightarrow x^{k(p-1)(q-1)} - 1 \equiv 0 \bmod p$

$\equiv 1^{(q-1)k} \equiv 1 \bmod p$

$x^{k(p-1)(q-1)} \bmod q$

$\equiv 1^{k(p-1)} \equiv 1 \bmod q \Rightarrow x^{k(p-1)(q-1)} - 1 \equiv 0 \bmod q$

$p \mid (x^{k(p-1)(q-1)} - 1)$

$q \mid (x^{k(p-1)(q-1)} - 1)$

$\Rightarrow pq \mid (x^{k(p-1)(q-1)} - 1)$

$5 \mid 70$

$7 \mid 70$

$35 \mid 70$

$x^{k(p-1)(q-1)} - 1 \equiv 0 \bmod pq$ (N)

$\Rightarrow x^{k(p-1)(q-1)} \equiv 1 \bmod N$

$\Rightarrow x^{k(p-1)(q-1)} x^1 \equiv x \bmod N \Rightarrow x^{k(p-1)(q-1)+1} \equiv x \bmod N$ (anything)

$x^{ed} \bmod N \equiv x \bmod N$

$ed \equiv k(p-1)(q-1)+1 \bmod (p-1)(q-1)$

$\Rightarrow ed \equiv 1 \bmod (p-1)(q-1)$

$\Rightarrow d \equiv e^{-1} \bmod (p-1)(q-1)$

$3^{-1} \bmod 64$

$3^{-1} \bmod 64$

$(1)64 + (-21)3 = 1$

$-21 \equiv 3^{-1} \bmod 64$

$\equiv 43$

$(1)65 + (-21)3 = 2$

$\Rightarrow (1)65 + (-22)3 = -1$

$\Rightarrow (2)65 + (-43)3 = 1$

65

-43

$22 \equiv 3^{-1} \bmod 65$

$24^{43} \mod 85$

$x \equiv a_1 \mod 5$

$x \equiv a_2 \mod 17$

$24^{43} \mod 5$

$\equiv (-1)^{43} \equiv -1 \equiv 4 \mod 5$

$-1^2 \equiv 4^2 \equiv 16 \equiv 1$

$-1^3 \equiv 4^3 \equiv 64 \equiv 4 \equiv -1$

$24^{43} \mod 17$

$\equiv 7^{43}$

$\equiv (7^2)^{21} \cdot 7$

$\equiv (-2)^{21} \cdot 7$

$49 \equiv -2 \mod 17$

$16 \equiv -1 \mod 17$

$\equiv ((-2)^4)^5 \cdot (-2) \cdot 7$

$\equiv (-1)^5 \cdot (-2) \cdot 7$

$\equiv 14 \mod 17$

$b_2 = p(p^{-1} \mod q) \equiv 5 \cdot 7 \equiv 35$

$b_1 = q(q^{-1} \mod p) \equiv 17 \cdot 3 \equiv 51$

$5^{-1} \mod 17 \equiv 7$

$17^{-1} \mod 5 \equiv 2^{-1} \mod 5 \equiv 3$

$x \equiv 4 \cdot 51 + 14 \cdot 35 \mod 85$

$\equiv 204 + 490$

$\equiv 694 \mod 85$

$\equiv \boxed{14} \mod 85$

510

170

680

(f) Suppose Bob receives the message $y = 24$ from Alice. What equation would he use to decrypt the message? What is the decrypted message?

$24^{43} \mod 85$

$24^{43} \mod 5$

$24^{43} \mod 17$

$x \equiv a \mod 5$

$x \equiv b \mod 17$

2 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p, q, r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$.

3 RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all

of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(N_1, e), \ldots, (N_k, e)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

(a) Suppose Eve sees the public keys $(p_1q_1, 7)$ and $(p_1q_2, 7)$ as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve cannot compute prime factors efficiently. Think of p_1, q_1, q_2 as massive 1024-bit numbers. Assume p_1, q_1, q_2 are all distinct and are valid primes for RSA to be carried out.

(b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(p_1q_1, 3)$, $(p_2q_2, 3)$, and $(p_3q_3, 3)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above. Assume $p_1, p_2, p_3, q_1, q_2, q_3$ are all distinct and are valid primes for RSA to be carried out.

(c) Let's say the secret x was not changed ($e = 3$), so they used the same public keys as before, but did not transmit different messages. How can Eve figure out x?