Asymmetric Ciphers

Dr. Chuck Rocca
roccac@wcsu.edu
http://sites.wcsu.edu/roccac

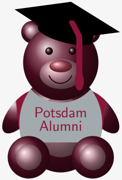

Table of Contents

Symmetric Cipher

Definition (Symmetric Cipher)

In a *symmetric cipher* the sender Alice and recipient Bob have equal knowledge of a key allowing them both to encipher and or decipher a message. Examples of these include affine ciphers, Vigenere's Cipher, Vernam's Cipher, Hill's Cipher, DES, and AES.

Asymmetric

Definition (Asymmetric Cipher)

In an *asymmetric cipher* the sender Alice makes use of a key, possibly public, to a trap-door function and the recipient Bob then uses a secret key known only to him to decipher. So their knowledge is not equal. Examples of this include RSA, Diffie-Hellman Key Exchange, ElGamal, Elliptic Curve, and Lattice Based encryption.

Table of Contents

Factors

Theorem (Fundamental Theorem of Arithmetic)

Given an integer $n \in \mathbb{N}$, either n is prime or n may be written as a product of primes

$$n = p_1 p_2 p_3 \cdots p_k$$

which is unique up to order.

Primitive Roots

Definition (Primitive Roots)

Given a natural number n, we say that $a \in \mathbb{N}$ is a primitive root of n if the powers

$$a^1, a^2, a^3, \ldots, a^{\phi(n)}$$

is a reduced residue system modulo n. We will see later that $a = 3$ is a primitive root for $n = 31$, i.e. modulo 31

$$\{3, 3^2, \ldots, 3^{30}\} = \{1, 2, 3, 4, \ldots, 30\}.$$

Primitive Roots

Definition (Primitive Roots)

Given a natural number n, we say that $a \in \mathbb{N}$ is a primitive root of n if the powers

$$a^1, a^2, a^3, \dots, a^{\phi(n)}$$

is a reduced residue system modulo n. We will see later that $a = 3$ is a primitive root for $n = 31$, i.e. modulo 31

$$\{3, 3^2, \dots, 3^{30}\} = \{1, 2, 3, 4, \dots, 30\}.$$

Theorem

A positive integer $n > 1$, has a primitive root if and only if $n = 2, 4, p^t,$ or $2p^t$ where p is an odd prime and t is a positive integer.

Logs

Definition (Discrete Logarithm Problem)

Let a be a primitive root in $\mathbb{F}_p$ for a prime p and let h be a non-zero element of $\mathbb{F}_p$. The *Discrete Logarithm Problem (DLP)* is the problem of finding x such that

$$a^x \equiv h \pmod{p}.$$

The number x is called the discrete logarithm of h to the base a and is denoted $\log_a(h)$.

Table of Contents

Diffie-Hellman Key Exchange

Alice | **Bob**

Publicly pick p and g with large prime order mod p

Privately picks a, send $A \equiv g^a \pmod{p}$

Privately picks b, send $B \equiv g^b \pmod{p}$

Calculate $B^a \equiv g^{ab} \pmod{p}$

Calculate $A^b \equiv g^{ab} \pmod{p}$

Private Key $\equiv g^{ab} \pmod{p}$

Diffie-Hellman Key Exchange

Alice | **Bob**

Publicly pick p and g with large prime order mod p

Alice: Privately picks a, send $A \equiv g^a \pmod{p}$

Bob: Privately picks b, send $B \equiv g^b \pmod{p}$

Alice: Calculate $B^a \equiv g^{ab} \pmod{p}$

Bob: Calculate $A^b \equiv g^{ab} \pmod{p}$

Private Key $\equiv g^{ab} \pmod{p}$

Diffie-Hellman Key Exchange

Alice | **Bob**

Publicly pick p and g with large prime order mod p

Alice: Privately picks a, send $A \equiv g^a \pmod{p}$

Bob: Privately picks b, send $B \equiv g^b \pmod{p}$

Alice: Calculate $B^a \equiv g^{ab} \pmod{p}$

Bob: Calculate $A^b \equiv g^{ab} \pmod{p}$

Private Key $\equiv g^{ab} \pmod{p}$

Diffie-Hellman Key Exchange

Alice | **Bob**

Publicly pick p and g with large prime order mod p

Privately picks a, send $A \equiv g^a \pmod{p}$

Privately picks b, send $B \equiv g^b \pmod{p}$

Calculate $B^a \equiv g^{ab} \pmod{p}$

Calculate $A^b \equiv g^{ab} \pmod{p}$

Private Key $\equiv g^{ab} \pmod{p}$

Diffie-Hellman Key Exchange

Alice

Bob

Publicly pick p and g with large prime order mod p

Privately picks a, send $A \equiv g^a \pmod{p}$

Privately picks b, send $B \equiv g^b \pmod{p}$

Calculate $B^a \equiv g^{ab} \pmod{p}$

Calculate $A^b \equiv g^{ab} \pmod{p}$

Private Key $\equiv g^{ab} \pmod{p}$

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:										
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3									
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9								
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod p$:	3	9	27							
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod p$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod p$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19						
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26					
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16				
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17			
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20		
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:										
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13									
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8								
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod p$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod p$:	13	8	24							
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod p$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10						
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30					
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28				
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22			
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod p$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod p$:	13	8	24	10	30	28	22	4		
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod p$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:										

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:	15									

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod p$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod p$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod p$:	15	14								

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:	15	14	11							

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:	15	14	11	2						

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:	15	14	11	2	6					

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:	15	14	11	2	6	18				

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:	15	14	11	2	6	18	23			

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:	15	14	11	2	6	18	23	7		

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:	15	14	11	2	6	18	23	7	21	

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod p$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod p$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod p$:	15	14	11	2	6	18	23	7	21	1

Picking g

Let's see that 3 is a primitive root modulo $p = 31$.

i:	1	2	3	4	5	6	7	8	9	10
$a^i \pmod{p}$:	3	9	27	19	26	16	17	20	29	25
i:	11	12	13	14	15	16	17	18	19	20
$a^i \pmod{p}$:	13	8	24	10	30	28	22	4	12	5
i:	21	22	23	24	25	26	27	28	29	30
$a^i \pmod{p}$:	15	14	11	2	6	18	23	7	21	1

Let's let $g = 3^6 \pmod{31} = 16$ which has order 5 (pretend 5 is big)

Now the a, the b, and the *private key*

- Note that $a, b < 5$, the order of 16 modulo 31

Now the *a*, the *b*, and the *private key*

- Note that $a, b < 5$, the order of 16 modulo 31
- Alice picks $a = 3$ so that

$$A \equiv g^a \equiv 4 \pmod{31}$$

Now the *a*, the *b*, and the *private key*

- Note that $a, b < 5$, the order of 16 modulo 31
- Alice picks $a = 3$ so that

$$A \equiv g^a \equiv 4 \pmod{31}$$

- Bob picks $b = 4$ so that

$$B \equiv g^b \equiv 2 \pmod{31}$$

Now the *a*, the *b*, and the *private key*

- Note that $a, b < 5$, the order of 16 modulo 31
- Alice picks $a = 3$ so that

$$A \equiv g^a \equiv 4 \pmod{31}$$

- Bob picks $b = 4$ so that

$$B \equiv g^b \equiv 2 \pmod{31}$$

- The *private key* is then

$$A^b \equiv B^a \equiv g^{ab} = 8 \pmod{31}$$

Table of Contents

ElGamal Crypto System

Alice

Publicly pick p and g
with large prime order
mod p, privately pick a,
calculate $A \equiv g^a \pmod{p}$

Alice's Public Key (p, g, A)

Bob

With message m calculate
and send $c_1 \equiv g^k \pmod{p}$
and $c_2 \equiv m\,A^k \pmod{p}$
for random disposable k

Calculate

$$\begin{aligned}(c_1)^{-a} c_2 &\equiv g^{-ak} m A^k \\ &\equiv g^{-ak} m g^{ak} \\ &\equiv m \pmod{p}\end{aligned}$$

ElGamal Crypto System

Alice

Publicly pick p and g with large prime order mod p, privately pick a, calculate $A \equiv g^a \pmod{p}$

Alice's Public Key (p, g, A)

Bob

With message m calculate and send $c_1 \equiv g^k \pmod{p}$ and $c_2 \equiv m\,A^k \pmod{p}$ for random disposable k

Calculate

$$\begin{aligned} (c_1)^{-a} c_2 &\equiv g^{-ak} m A^k \\ &\equiv g^{-ak} m g^{ak} \\ &\equiv m \pmod{p} \end{aligned}$$

ElGamal Crypto System

Alice

Publicly pick p and g with large prime order mod p, privately pick a, calculate $A \equiv g^{a} \pmod{p}$

Alice's Public Key (p, g, A)

Bob

With message m calculate and send $c_1 \equiv g^{k} \pmod{p}$ and $c_2 \equiv m\,A^{k} \pmod{p}$ for random disposable k

Calculate

$$
\begin{aligned}
(c_1)^{-a} c_2 &\equiv g^{-ak} m A^{k} \\
&\equiv g^{-ak} m g^{ak} \\
&\equiv m \pmod{p}
\end{aligned}
$$

ElGamal Crypto System

Alice

Publicly pick p and g with large prime order mod p, privately pick a, calculate $A \equiv g^a \pmod{p}$

Alice's Public Key (p, g, A)

Bob

With message m calculate and send $c_1 \equiv g^k \pmod{p}$ and $c_2 \equiv m\,A^k \pmod{p}$ for random disposable k

Calculate

$$\begin{aligned}(c_1)^{-a} c_2 &\equiv g^{-ak} m A^k \\ &\equiv g^{-ak} m g^{ak} \\ &\equiv m \pmod{p}\end{aligned}$$

ElGamal Crypto System

Alice

Publicly pick p and g with large prime order mod p, privately pick a, calculate $A \equiv g^a \pmod{p}$

Alice's Public Key (p, g, A)

Bob

With message m calculate and send $c_1 \equiv g^k \pmod{p}$ and $c_2 \equiv m\,A^k \pmod{p}$ for random disposable k

Calculate

$$\begin{aligned}(c_1)^{-a} c_2 &\equiv g^{-ak} m A^k \\ &\equiv g^{-ak} m g^{ak} \\ &\equiv m \pmod{p}\end{aligned}$$

Encryption Example

- Use $p = 31$, $g = 16$ (which has order 5), and $a = 3$

Encryption Example

- Use $p = 31$, $g = 16$ (which has order 5), and $a = 3$
- Public Key $(p, g, A) = (31, 16, 4)$, with $A \equiv g^a \pmod{p}$

Encryption Example

- Use $p = 31$, $g = 16$ (which has order 5), and $a = 3$
- Public Key $(p, g, A) = (31, 16, 4)$, with $A \equiv g^a \pmod{p}$
- Bob "randomly" chooses $k = 4$ to encipher "T"=19,

$$c_1 = g^k \equiv 2 \pmod{31} \text{ and}$$

$$c_2 = \text{“T”} A^k \equiv 19 \cdot 4^4 \equiv 28 \pmod{31}$$

Decryption Example

- ${c_1}^{-a} \equiv 2^{-3} \equiv (2^3)^{-1} \equiv 4 \pmod{31}$

Decryption Example

- $c_1^{-a} \equiv 2^{-3} \equiv (2^3)^{-1} \equiv 4 \pmod{31}$
- $c_1^{-a} c_2 \equiv 4 \cdot 28 \equiv 19 \pmod{31}$

Decryption Example

- ${c_1}^{-a} \equiv 2^{-3} \equiv (2^3)^{-1} \equiv 4 \pmod{31}$
- ${c_1}^{-a} c_2 \equiv 4 \cdot 28 \equiv 19 \pmod{31}$
- 19= "T"

Table of Contents

RSA Crypto System

Alice

Privately pick primes p and q of similar magnitude, let $N = pq$. Pick e and d so that $ed \equiv 1 \pmod{\phi(N)}$, publish (e, N)

Alice's Public Key (e, N)

Bob

With message m calculate and send $c \equiv m^e \pmod{N}$

Calculate

$$\begin{aligned} c^d &\equiv m^{ed} \\ &\equiv m^{\phi(N)k+1} \\ &\equiv \left(m^{\phi(N)}\right)^k m \\ &\equiv 1^k m \\ &\equiv m \pmod{N} \end{aligned}$$

RSA Crypto System

Alice

Privately pick primes p and q of similar magnitude, let $N = pq$. Pick e and d so that $ed \equiv 1 \pmod{\phi(N)}$, publish (e, N)

Alice's Public Key (e, N)

Bob

With message m calculate and send $c \equiv m^e \pmod{N}$

Calculate

$$\begin{aligned} c^d &\equiv m^{ed} \\ &\equiv m^{\phi(N)k+1} \\ &\equiv \left(m^{\phi(N)}\right)^k m \\ &\equiv 1^k m \\ &\equiv m \pmod{N} \end{aligned}$$

RSA Crypto System

Alice

Privately pick primes p and q of similar magnitude, let $N = pq$. Pick e and d so that $ed \equiv 1 \pmod{\phi(N)}$, publish (e, N)

Alice's Public Key (e, N)

Bob

With message m calculate and send $c \equiv m^e \pmod{N}$

Calculate

$$\begin{aligned} c^d &\equiv m^{ed} \\ &\equiv m^{\phi(N)k+1} \\ &\equiv \left(m^{\phi(N)}\right)^k m \\ &\equiv 1^k m \\ &\equiv m \pmod{N} \end{aligned}$$

RSA Crypto System

Alice

Privately pick primes p and q of similar magnitude, let $N = pq$. Pick e and d so that $ed \equiv 1 \pmod{\phi(N)}$, publish (e, N)

Alice's Public Key (e, N)

Bob

With message m calculate and send $c \equiv m^e \pmod{N}$

Calculate

$$
\begin{aligned}
c^d &\equiv m^{ed} \\
&\equiv m^{\phi(N)k+1} \\
&\equiv \left(m^{\phi(N)}\right)^k m \\
&\equiv 1^k m \\
&\equiv m \pmod{N}
\end{aligned}
$$

RSA Crypto System

Alice

Privately pick primes p and q of similar magnitude, let $N = pq$. Pick e and d so that $ed \equiv 1 \pmod{\phi(N)}$, publish (e, N)

Alice's Public Key (e, N)

Bob

With message m calculate and send $c \equiv m^e \pmod{N}$

Calculate

$$\begin{aligned} c^d &\equiv m^{ed} \\ &\equiv m^{\phi(N)k+1} \\ &\equiv \left(m^{\phi(N)}\right)^k m \\ &\equiv 1^k m \\ &\equiv m \pmod{N} \end{aligned}$$

RSA Crypto System

Alice

Bob

Privately pick primes p and q of similar magnitude, let $N = pq$. Pick e and d so that $ed \equiv 1 \pmod{\phi(N)}$, publish (e, N)

Alice's Public Key (e, N)

With message m calculate and send $c \equiv m^e \pmod{N}$

Calculate

$$\begin{aligned} c^d &\equiv m^{ed} \\ &\equiv m^{\phi(N)k+1} \\ &\equiv \left(m^{\phi(N)}\right)^k m \\ &\equiv 1^k m \\ &\equiv m \pmod{N} \end{aligned}$$

Technically we applied Euler's Theorem with moduli p and q, not N, and then used the Chinese Remainder Theorem to stitch the answers together, this allows us to encipher any $0 \le m < N$.

Key Generation

- Choose $p = 31$ and $q = 37$

Key Generation

- Choose $p = 31$ and $q = 37$
- $N = p \cdot q = 1147$ and $\phi(1147) = \phi(31)\phi(37) = 30 \cdot 36 = 1080$

Key Generation

- Choose $p = 31$ and $q = 37$
- $N = p \cdot q = 1147$ and $\phi(1147) = \phi(31)\phi(37) = 30 \cdot 36 = 1080$
- $1080 = 2^3 \cdot 3^3 \cdot 5$, let $e = 101$

Key Generation

- Choose $p = 31$ and $q = 37$
- $N = p \cdot q = 1147$ and $\phi(1147) = \phi(31)\phi(37) = 30 \cdot 36 = 1080$
- $1080 = 2^3 \cdot 3^3 \cdot 5$, let $e = 101$
- $d = 101^{-1} \pmod{1080} = 941$, $941 \cdot 101 = 88 \cdot 1080 + 1$

Key Generation

- Choose $p = 31$ and $q = 37$
- $N = p \cdot q = 1147$ and $\phi(1147) = \phi(31)\phi(37) = 30 \cdot 36 = 1080$
- $1080 = 2^3 \cdot 3^3 \cdot 5$, let $e = 101$
- $d = 101^{-1} \pmod{1080} = 941$, $941 \cdot 101 = 88 \cdot 1080 + 1$
- Publish (101,1147)

Encryption Example

- Message "T"$=19$

Encryption Example

- Message "T"=19
- $c \equiv 19^{101} \pmod{1147} = 165$

Encryption Example

- Message "T"=19
- $c \equiv 19^{101} \pmod{1147} = 165$
- Send 165

Decryption Examples

- Cipher Message 165

Decryption Examples

- Cipher Message 165
- $m \equiv 165^{941} \pmod{31} = 19$

Decryption Examples

- Cipher Message 165
- $m \equiv 165^{941} \pmod{31} = 19$
- $m \equiv 165^{941} \pmod{37} = 19$

Decryption Examples

- Cipher Message 165
- $m \equiv 165^{941} \pmod{31} = 19$
- $m \equiv 165^{941} \pmod{37} = 19$
- Using the Chinese Remainder Theorem we then get

$$m \equiv 165^{941} \pmod{1147} = 19$$

Decryption Examples

- Cipher Message 165
- $m \equiv 165^{941} \pmod{31} = 19$
- $m \equiv 165^{941} \pmod{37} = 19$
- Using the Chinese Remainder Theorem we then get

$$m \equiv 165^{941} \pmod{1147} = 19$$

- The CRT is used because it is not necessary that $gcd(m, N) = 1$ only that $m < N$.

Decryption Examples

- Cipher Message 165
- $m \equiv 165^{941} \pmod{31} = 19$
- $m \equiv 165^{941} \pmod{37} = 19$
- Using the Chinese Remainder Theorem we then get

$$m \equiv 165^{941} \pmod{1147} = 19$$

- The CRT is used because it is not necessary that $gcd(m, N) = 1$ only that $m < N$.
- 19= "T"

Example with Non-Relatively Prime Message

- Start with the same keys: $p = 31$, $q = 37$, $N = 1147$, $\phi(N) = 1080$, $e = 101$, and $d = 941$

Example with Non-Relatively Prime Message

- Start with the same keys: $p = 31$, $q = 37$, $N = 1147$, $\phi(N) = 1080$, $e = 101$, and $d = 941$
- The "message" $m = 93$ is not relatively prime to N, $gcd(m, N) = p$, technically we can't apply Euler's Theorem with N

Example with Non-Relatively Prime Message

- Start with the same keys: $p = 31$, $q = 37$, $N = 1147$, $\phi(N) = 1080$, $e = 101$, and $d = 941$
- The "message" $m = 93$ is not relatively prime to N, $gcd(m, N) = p$, technically we can't apply Euler's Theorem with N
- Enciphering m gives $c \equiv m^e \pmod{N} = 868$

Example with Non-Relatively Prime Message

- Start with the same keys: $p = 31$, $q = 37$, $N = 1147$, $\phi(N) = 1080$, $e = 101$, and $d = 941$
- The "message" $m = 93$ is not relatively prime to N, $gcd(m, N) = p$, technically we can't apply Euler's Theorem with N
- Enciphering m gives $c \equiv m^e \pmod{N} = 868$
- Next decipher with respect to p and q

Example with Non-Relatively Prime Message

- Start with the same keys: $p = 31$, $q = 37$, $N = 1147$, $\phi(N) = 1080$, $e = 101$, and $d = 941$
- The "message" $m = 93$ is not relatively prime to N, $gcd(m, N) = p$, technically we can't apply Euler's Theorem with N
- Enciphering m gives $c \equiv m^e \pmod{N} = 868$
- Next decipher with respect to p and q
    - $m_1 \equiv c^d \pmod{p} = 0$

Example with Non-Relatively Prime Message

- Start with the same keys: $p = 31$, $q = 37$, $N = 1147$, $\phi(N) = 1080$, $e = 101$, and $d = 941$
- The "message" $m = 93$ is not relatively prime to N, $gcd(m, N) = p$, technically we can't apply Euler's Theorem with N
- Enciphering m gives $c \equiv m^e \pmod{N} = 868$
- Next decipher with respect to p and q
  - $m_1 \equiv c^d \pmod{p} = 0$
  - $m_2 \equiv c^d \pmod{q} = 19$ which is m modulo q

Example with Non-Relatively Prime Message

- Start with the same keys: $p = 31$, $q = 37$, $N = 1147$, $\phi(N) = 1080$, $e = 101$, and $d = 941$
- The "message" $m = 93$ is not relatively prime to N, $gcd(m, N) = p$, technically we can't apply Euler's Theorem with N
- Enciphering m gives $c \equiv m^e \pmod{N} = 868$
- Next decipher with respect to p and q
  - $m_1 \equiv c^d \pmod{p} = 0$
  - $m_2 \equiv c^d \pmod{q} = 19$ which is m modulo q
- Stitching those together with the Chinese Remainder Theorem we get:

Example with Non-Relatively Prime Message

- Start with the same keys: $p = 31$, $q = 37$, $N = 1147$, $\phi(N) = 1080$, $e = 101$, and $d = 941$
- The "message" $m = 93$ is not relatively prime to N, $gcd(m, N) = p$, technically we can't apply Euler's Theorem with N
- Enciphering m gives $c \equiv m^e \pmod{N} = 868$
- Next decipher with respect to p and q
  - $m_1 \equiv c^d \pmod{p} = 0$
  - $m_2 \equiv c^d \pmod{q} = 19$ which is m modulo q
- Stitching those together with the Chinese Remainder Theorem we get:
  - $m \equiv m_1 \cdot q \cdot q' + m_2 \cdot p \cdot p' \pmod{N} = 93$ ✓

Example with Non-Relatively Prime Message

- Start with the same keys: $p = 31$, $q = 37$, $N = 1147$, $\phi(N) = 1080$, $e = 101$, and $d = 941$
- The "message" $m = 93$ is not relatively prime to N, $gcd(m, N) = p$, technically we can't apply Euler's Theorem with N
- Enciphering m gives $c \equiv m^e \pmod{N} = 868$
- Next decipher with respect to p and q
  - $m_1 \equiv c^d \pmod{p} = 0$
  - $m_2 \equiv c^d \pmod{q} = 19$ which is m modulo q
- Stitching those together with the Chinese Remainder Theorem we get:
  - $m \equiv m_1 \cdot q \cdot q' + m_2 \cdot p \cdot p' \pmod{N} = 93$ ✓
  - where $q' \equiv q^{-1} \pmod{p} = 26$ and $p' \equiv p^{-1} \pmod{q} = 6$

Table of Contents

Asymmetric Ciphers

Dr. Chuck Rocca
roccac@wcsu.edu

http://sites.wcsu.edu/roccac