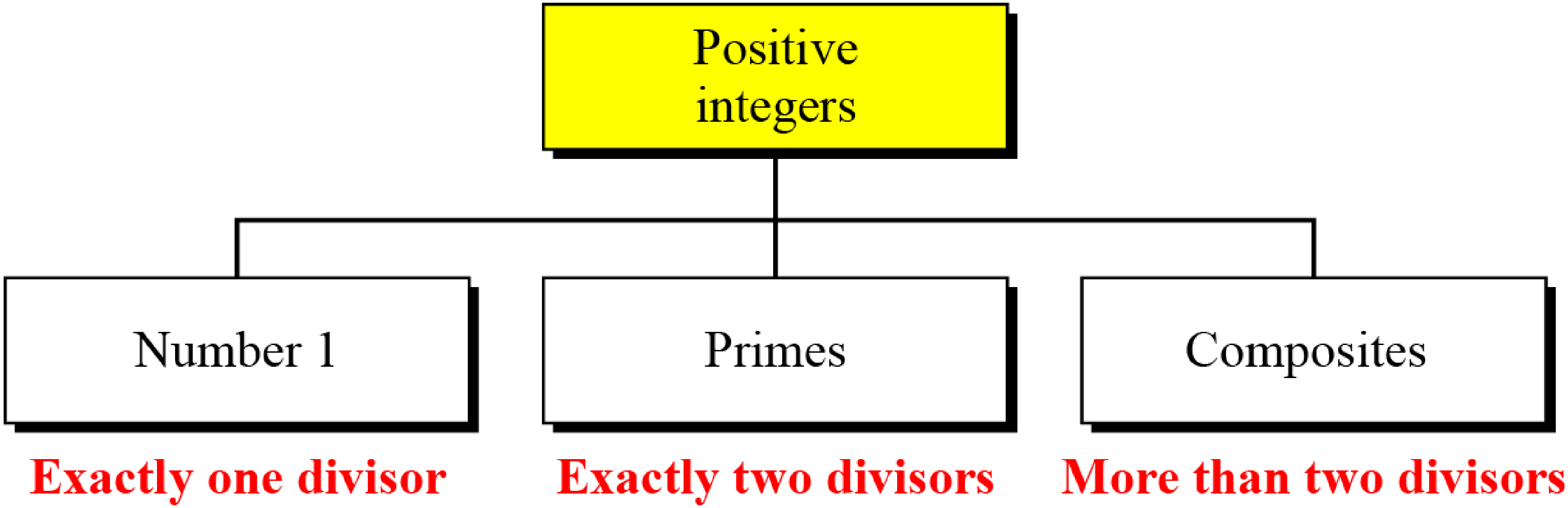
UNIT II
NUMBER THEORY AND PUBLIC KEY CRYPTOGRAPHY

INTRODUCTION TO NUMBER THEORY

Ref:Cryptography and Network Security by Behrouz Forouzan

Three groups of positive integers



A prime is divisible only by itself and 1.

Checking for Primeness

Given a number n, how can we determine if n is a prime? The answer is that we need to see if the number is divisible by all primes less than $\sqrt{n}$

Is 97 a prime?

Solution

The floor of $\sqrt{97} = 9$. The primes less than 9 are 2, 3, 5, and 7. We need to see if 97 is divisible by any of these numbers. It is not, so 97 is a prime.

Is 301 a prime?

Solution

The floor of $\sqrt{301} = 17$. We need to check 2, 3, 5, 7, 11, 13, and 17. The numbers 2, 3, and 5 do not divide 301, but 7 does. Therefore 301 is not a prime.

Sieve of Eratosthenes

https://commons.wikimedia.org/wiki/File:Sieve_of_Eratosthenes_animation.gif#/media/File:Sieve_of_Eratosthenes_animation.gif

Sieve of Eratosthenes

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Euler's Phi-Function

- *Euler's phi-function, ϕ (n), which is sometimes called the Euler's totient function plays a very important role in cryptography. The function finds the number of integers that are both smaller than n and relatively prime to n*

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

Find the GCD(HCF) of

1)12&13

2)12&15

3)36&60

Example

1.What is the value of $\Phi(13)$?

Solution

Because 13 is a prime, $\Phi(13) = (13 - 1) = 12$.

2.What is the value of $\Phi(10)$?

Solution

We can use the third rule:

$\phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4$, because 2 and 5 are primes.

3.What is the value of $\phi(240)$?

$\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

Solution

4. Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$?

Solution

3.We can write $240 = 2^4 \times 3^1 \times 5^1$.

Then $\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0) = 64$

4. No. The third rule applies when m and n are relatively

prime. Here $49 = 7^2$. We need to use the fourth rule:

$\phi(49) = 7^2 - 7^1 = 42$.

5.What is the number of elements in Z_{14}^*

Solution:

$\Phi(14) = \phi(2) \times \phi(7) = 1 \times 6 = 6$

The members are 1,3,5,7,11,13

UNIT II
NUMBER THEORY AND PUBLIC KEY CRYPTOGRAPHY

INTRODUCTION TO NUMBER THEORY-LECTURE 2

Ref:Cryptography and Network Security by Behrouz Forouzan

Fermat's Little Theorem

- First Version

$$\boxed{a^{p-1} \equiv 1 \bmod p}$$

- Second Version

$$\boxed{a^{p} \equiv a \bmod p}$$

Examples

1.Find the result of 6^{10} mod 11.

Solution

We have 6^{10} mod 11 = 1. This is the first version of Fermat's little theorem where $p = 11$.

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

2. Find the result of 3^{12} mod 11.

Solution

Here the exponent (12) and the modulus (11) are not the same. With substitution this can be solved using Fermat's little theorem.

$a^p \equiv a \bmod p$

$$3^{12} \bmod 11 = (3^{11} \times 3) \bmod 11 = (3^{11} \bmod 11)\,(3 \bmod 11) = (3 \times 3) \bmod 11 = 9$$

Multiplicative Inverses

- Find the multiplicative inverse of 8 mod 11, using the Euclidean Algorithm.

gcd(8, 11) = 1

11 = 8(1) + 3

8 = 3(2) + 2

3 =2(1) + 1

Now reverse the process using the equations

1 = 3 − 2(1)

1 = 3 − (8 − 3(2))(1) = 3 − (8 − (3(2)) = 3(3) − 8

1 = (11 − 8(1))(3) − 8 = 11(3) − 8(4) = 11(3) + 8(−4)

Therefore 1 ≡ 8(−4) mod 11, or if we prefer a residue value for the multiplicative inverse, 1 ≡ 8(7) mod 11.

Work at home

- Find the multiplicative inverses of the following:

1) 50 mod 71

2) 43 mod 64

Euler's Theorem

- *First Version: If a and n are coprime then*

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$$

Second Version: similar to first version but removes the condition that a and n should be prime

$$\boxed{a^{k \times \phi(n) + 1} \equiv a \pmod{n}}$$

The second version of Euler's theorem is used in the RSA cryptosystem

Euler's Phi-Function

To Remember:

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

Examples

1.Find the result of 6^{24} mod 35.

Solution

We have $6^{24} \bmod 35 = 6^{\phi(35)} \bmod 35 = 1$.

2. Find the result of 20^{62} mod 77

Solution

If we let $k = 1$ on the second version, we have

$$20^{62} \bmod 77 = (20 \bmod 77)\,(20^{\phi(77)\,+\,1} \bmod 77) \bmod 77$$

$$= (20)(20) \bmod 77 = 15.$$

PRIMALITY TESTING

- Deterministic Algorithms
- Probabilistic Algorithms
- Recommended Primality Test

Deterministic Algorithms

Divisibility Algorithm

Algorithm *Pseudocode for the divisibility test*

```
Divisibility_Test (n)                    // n is the number to test for primality
{
  r ← 2
  while (r < √n )
  {
   if (r | n) return "a composite"
   r ← r + 1
  }
  return "a prime"
}
```

AKS algorithm

The AKS primality test (also known as Agrawal–Kayal–Saxena primality test and cyclotomic AKS test) is a deterministic algorithm created and published by , computer scientists at the Indian Institute of Technology Kanpur, on August 6, 2002

Probabilistic Algorithms

- *Fermat Test*

$$\boxed{\textbf{If } n \textbf{ is a prime, then } a^{n-1} \equiv 1 \bmod n.}$$

If n is a prime, $a^{n-1} \equiv 1 \bmod n$

If n is a composite, it is possible that $a^{n-1} \equiv 1 \bmod n$

Does the number 561 pass the Fermat test?

Solution

Use base 2

$$2^{561-1} = 1 \bmod 561$$

The number passes the Fermat test, but it is not a prime, because 561 = 33 × 17.

Square Root Test

If n is a prime, $\sqrt{1} \bmod n = \pm 1$.
If n is a composite, $\sqrt{1} \bmod n = \pm 1$ and possibly other values.

What are the square roots of 1 mod n if n is 7 (a prime)?

Solution

The only square roots are 1 and −1. We can see that

$$1^2 = 1 \bmod 7 \qquad (-1)^2 = 1 \bmod 7$$
$$2^2 = 4 \bmod 7 \qquad (-2)^2 = 4 \bmod 7$$
$$3^2 = 2 \bmod 7 \qquad (-3)^2 = 2 \bmod 7$$

Note that we don't have to test 4, 5 and 6 because 4 = –3 mod 7, 5 = –2 mod 7 and 6 = –1 mod 7.

What are the square roots of 1 mod n if n is 22 (a composite)?

Solution

Surprisingly, there are only two solutions, +1 and −1, although 22 is a composite.

$$1^2 = 1 \bmod 22$$
$$(-1)^2 = 1 \bmod 22$$

- *Miller-Rabin Test*

$$n - 1 = m \times 2^k$$

Idea behind Fermat primality test

$$a^{n-1} = a^{m \times 2^k} = [a^m]^{2^k} = [a^m]^{\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{k \text{ times}}}$$

Algorithm *Pseudocode for Miller-Rabin test*

```
Miller_Rabin_Test (n, a)                          // n is the number; a is the base.
{
    Find m and k such that n − 1 = m × 2^k
    T ← a^m mod n
    if (T = ± 1)   return "a prime"
    for (i ← 1 to k − 1)                          // k − 1 is the maximum number of steps.
    {
        T ← T^2 mod n
        if (T = +1) return "a composite"
        if (T = −1) return "a prime"
    }
    return "a composite"
}
```

Does the number 561 pass the Miller-Rabin test?

Solution

Using base 2, let $561 - 1 = 35 \times 2^4$, which means

$m = 35$, $k = 4$, and $a = 2$.

Initialization:	$T = 2^{35} \bmod 561 = 263 \bmod 561$	
$k = 1$:	$T = 263^2 \bmod 561 = 166 \bmod 561$	
$k = 2$:	$T = 166^2 \bmod 561 = 67 \bmod 561$	
$k = 3$:	$T = 67^2 \bmod 561 = +1 \bmod 561$	$\rightarrow$ **a composite**

Work at home

1.What are the square roots of 1mod n ,if n is 8?

2.What are the square roots of 1 mod n,if n is 17?

3.Check whether 61 passes Miller Rabin test

Recommended Primality Test

- *Today, one of the most popular primality test is a combination of the divisibility test and the Miller-Rabin test.*

UNIT II
NUMBER THEORY AND PUBLIC KEY CRYPTOGRAPHY

INTRODUCTION TO NUMBER THEORY-CRT

Ref:Cryptography and Network Security by Behrouz Forouzan

CHINESE REMAINDER THEOREM

The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime, as shown below:

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_k \pmod{m_k}
\end{aligned}
$$

- Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \dots \times m_k$. This is the common modulus.

2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.

3. Find the multiplicative inverse of $M_1, M_2, \dots, M_k$ using corresponding moduli $(m_1, m_2, \dots, m_k)$.Call the inverses

$$M_1^{-1}, M_2^{-1}, \dots, M_k^{-1}.$$

4. The solution to the simultaneous equations is

$$\boxed{x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M}$$

Example

Find the solution to the simultaneous equations:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

Solution

We follow the four steps.

1. $M = 3 \times 5 \times 7 = 105$

2. $M_1 = 105 / 3 = 35$, $M_2 = 105 / 5 = 21$, $M_3 = 105 / 7 = 15$

3. The inverses are $M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$

4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

   $= 23 \bmod 105$

Work at home

1. $x \equiv 3 \bmod 5$

   $x \equiv 1 \bmod 7$

   $x \equiv 6 \bmod 8$

UNIT II
NUMBER THEORY AND PUBLIC KEY CRYPTOGRAPHY

INTRODUCTION TO NUMBER THEORY-Quadratic Congruence_LECTURE 7

Ref:Cryptography and Network Security by Behrouz Forouzan

QUADRATIC CONGRUENCE

In cryptography, we also need to discuss quadratic congruence—that is, equations of the Form $a_2x^2 + a_1x + a_0 \equiv 0 \pmod{n}$. *We limit our discussion to quadratic equations in which* $a_2 = 1$ *and* $a_1 = 0$, *that is equations of the form*

$$\boxed{x^2 \equiv a \pmod{n}.}$$

How do you solve congruences of the form $x^2 \equiv a \pmod{m}$? *Said another way, how do you find square roots in modular arithmetic?*

Simple Example

We start off with a simple example.

Calculate x^2 modulo $m = 11$ for $x = 0, 1, 2, \cdots, 10$.

$$0^2 \equiv 0 \pmod{11}$$
$$1^2 \equiv 1 \pmod{11}$$
$$2^2 \equiv 4 \pmod{11}$$
$$3^2 \equiv 9 \pmod{11}$$
$$4^2 \equiv 5 \pmod{11}$$
$$5^2 \equiv 3 \pmod{11}$$
$$6^2 \equiv 3 \pmod{11}$$
$$7^2 \equiv 5 \pmod{11}$$
$$8^2 \equiv 9 \pmod{11}$$
$$9^2 \equiv 4 \pmod{11}$$
$$10^2 \equiv 1 \pmod{11}$$

The above calculation shows that the values of x^2 modulo $m = 11$ can only be $1, 3, 4, 5, 9$. So equations such as $x^2 \equiv a \pmod{11}$ for $a = 1, 3, 4, 5, 9$ have solutions. For example, the solutions for the equation $x^2 \equiv 5 \pmod{11}$ are $x = 4$ and $x = 7$.

Quadratic Congruence Modulo a Prime

- *We first consider the case in which the modulus is a prime*
- The equation $x^2 \equiv 3 \pmod{11}$ has two solutions, 5 and 6.
- The equation $x^2 \equiv 2 \pmod{11}$ has no solution. No integer x can be found such that its square is 2 mod 11.

- *Quadratic Residues and Nonresidue*
- If $x^2 \equiv a \pmod{n}$ has a solution, we say a is a "quadratic residue mod n." If this congruence has no solution, we say x is a "quadratic non-residue mod p.

- There are 10 elements in $Z_{11}*$. Exactly five of them are quadratic residues and five of them are nonresidues. In other words, $Z_{11}*$ is divided into two separate sets, QR and QNR

Division of $Z_{11}*$ elements into QRs and QNRs

$Z_{11}* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

QR set = $\{1, 3, 4, 5, 9\}$

Each element has a square root

QNR set = $\{2, 6, 7, 8, 10\}$

No element has a square root

Work at home

- Solve the following quadratic equations:

a. $x^2 \equiv 3 \pmod{23}$

b. $x^2 \equiv 2 \pmod{11}$

c. $x^2 \equiv 7 \pmod{19}$

- *Euler's Criterion*

a. *If* $a^{(p-1)/2} \equiv 1 \pmod{p}$, *a is a quadratic residue modulo p.*

b. *If* $a^{(p-1)/2} \equiv -1 \pmod{p}$, *a is a quadratic nonresidue modulo p.*

- To find out if 14 or 16 is a QR in Z_{23}^*, we calculate:

$14^{(23-1)/2} \bmod 23 \rightarrow 22 \bmod 23 \rightarrow -1 \bmod 23$ nonresidue

$16^{(23-1)/2} \bmod 23 \rightarrow 16^{11} \bmod 23 \rightarrow 1 \bmod 23$ residue

Quadratic Congruence Modulo a Composite

$$x^2 \equiv a \bmod (n)$$
$$n = p_1 \times p_2 \times \ . \ \ . \ \ . \times p_k$$

$$\longrightarrow$$

$$x^2 \equiv a_1 \pmod{p_1}$$
$$x^2 \equiv a_2 \pmod{p_1}$$
$$\bullet\bullet\bullet$$
$$x^2 \equiv a_k \pmod{p_k}$$

$$\longrightarrow$$

$$x_1 \equiv \pm\, b_1 \pmod{p_1}$$
$$x_2 \equiv \pm\, b_2 \pmod{p_1}$$
$$\bullet\bullet\bullet$$
$$x_\mathrm{k} \equiv \pm\, b_\mathrm{k} \pmod{p_k}$$

Quadratic Congruence Modulo a Composite

Assume that $x^2 \equiv 36 \pmod{77}$. We know that $77 = 7 \times 11$. We can write

$$x^2 \equiv 36 \pmod{7} \equiv 1 \pmod{7} \quad \text{and} \quad x^2 \equiv 36 \pmod{11} \equiv 3 \pmod{11}$$

The answers are $x \equiv +1 \pmod{7}$, $x \equiv -1 \pmod{7}$, $x \equiv +5 \pmod{11}$, and $x \equiv -5 \pmod{11}$. Now we can make four sets of equations out of these:

Set 1:	$x \equiv +1 \pmod{7}$	$x \equiv +5 \pmod{11}$
Set 2:	$x \equiv +1 \pmod{7}$	$x \equiv -5 \pmod{11}$
Set 3:	$x \equiv -1 \pmod{7}$	$x \equiv +5 \pmod{11}$
Set 4:	$x \equiv -1 \pmod{7}$	$x \equiv -5 \pmod{11}$

- How hard is it to solve a quadratic congruence modulo a composite? The main task is the factorization of the modulus. In other words, the complexity of solving a quadratic congruence modulo a composite is the same as factorizing a composite integer. As we have seen, if n is very large, factorization is infeasible.

UNIT II
NUMBER THEORY AND PUBLIC KEY CRYPTOGRAPHY

INTRODUCTION TO NUMBER THEORY-

Exponentiation and Logarithm_LECTURE 9

Ref:Cryptography and Network Security by Behrouz Forouzan

EXPONENTIATION AND LOGARITHM

Exponentiation: $y = a^x$ $\rightarrow$ **Logarithm:** $x = \log_a y$

Exponentiation

- *Fast Exponentiation:square-and-multiply method*

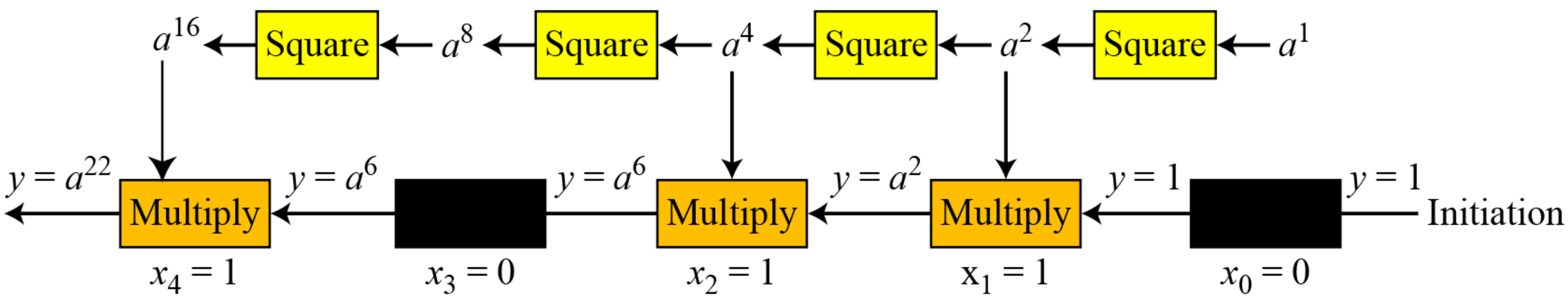
Algorithm *Pseudocode for square-and-multiply algorithm*

Square_and_Multiply (a, x, n)
{
  $y \leftarrow 1$
  for (i $\leftarrow$ 0 to $n_b - 1$) // n_b is the number of bits in x
  {
    if ($x_i = 1$) $y \leftarrow a \times y \mod n$ // multiply only if the bit is 1

    $a \leftarrow a^2 \mod n$ // squaring is not needed in the last iteration
  }
  return y
}

The process for calculating $y = a^x$ using the Algorithm is shown. (for simplicity, the modulus is not shown). In this case, $x = 22 = (10110)_2$ in binary. The exponent has five bits.

Demonstration of calculation of a^{22} using square-and-multiply method



DR MAHALINGAM MCET COLLEGE OF ENGINEERING AND TECHNOLOGY

Table *Calculation of 17^{22} mod 21*

i	x_i	*Multiplication* *(Initialization: $y = 1$)*	*Squaring* *(Initialization: $a = 17$)*
0	0	$\rightarrow$	$a = 17^2 \bmod 21 = 16$
1	1	$y = 1 \times 16 \bmod 21 = 16$ $\rightarrow$	$a = 16^2 \bmod 21 = 4$
2	1	$y = 16 \times 4 \bmod 21 = 1$ $\rightarrow$	$a = 4^2 \bmod 21 = 16$
3	0	$\rightarrow$	$a = 16^2 \bmod 21 = 4$
4	1	$y = 1 \times 4 \bmod 21 = 4$ $\rightarrow$	

```
}
```

NIA EDUCATIONAL INSTITUTIONS Enlightening Minds

Logarithm

- *Exhaustive Search*

Algorithm *Exhaustive search for modular logarithm*

```
Modular_Logarithm (a, y, n)
{
    for (x = 1 to n − 1)                    // k is the number of bits in x
    {
        if (y ≡ a^x mod n) return x
    }
    return failure
}
```

```
}
```

This is an inefficient algorithm as the complexity is exponential

- *Discrete Logarithm is the second approach*
- *Order of the Group*.
- What is the order of group $G = <Z_{21}*, \times>$? $|G| = \phi(21) = \phi(3) \times \phi(7) = 2 \times 6 = 12$. There are 12 elements in this group: 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, and 20. All are relatively prime with 21.

Order of an Element

- Find the order of all elements in $G = \langle Z_{10}^*, \times \rangle$.

Solution

This group has only $\phi(10) = 4$ elements: 1, 3, 7, 9. We can find the order of each element by trial and error.

a. $1^1 \equiv 1 \bmod (10) \rightarrow \text{ord}(1) = 1$.
b. $3^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(3) = 4$.
c. $7^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(7) = 4$.
d. $9^2 \equiv 1 \bmod (10) \rightarrow \text{ord}(9) = 2$.

a. $1^1 \equiv 1 \bmod (10) \rightarrow \text{ord}(1) = 1$.
b. $3^1 \equiv 3 \bmod (10)$; $3^2 \equiv 9 \bmod (10)$; $3^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(3) = 4$.
c. $7^1 \equiv 7 \bmod (10)$; $7^2 \equiv 9 \bmod (10)$; $7^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(7) = 4$.
d. $9^1 \equiv 9 \bmod (10)$; $9^2 \equiv 1 \bmod (10) \rightarrow \text{ord}(9) = 2$.

- *Primitive Roots* *In the group* $G = <Z_n{*}, \times>$, *when the order of an element is the same as* $\phi(n)$, *that element is called the primitive root of the group.*
- *Cyclic Group* *If g is a primitive root in the group, we can generate the set* $Z_n{*}$ *as* $Z_n{*} = \{g^1, g^2, g^3, \ldots, g^{\phi(n)}\}$

- The group $G = \langle Z_{10}^*, \times \rangle$ has two primitive roots. It can be found that the primitive roots are 3 and 7. The following shows how we can create the whole set Z_{10}^* using each primitive root.

$g = 3 \rightarrow$	$g^1 \bmod 10 = 3$	$g^2 \bmod 10 = 9$	$g^3 \bmod 10 = 7$	$g^4 \bmod 10 = 1$
$g = 7 \rightarrow$	$g^1 \bmod 10 = 7$	$g^2 \bmod 10 = 9$	$g^3 \bmod 10 = 3$	$g^4 \bmod 10 = 1$

The group $G = \langle Z_n^*, \times \rangle$ is a cyclic group if it has primitive roots.
The group $G = \langle Z_p^*, \times \rangle$ is always cyclic.

The idea of Discrete Logarithm

Properties of $G = \langle Z_p^*, \times \rangle$:

1.Its elements include all integers from 1 to $p - 1$.

2. It always has primitive roots.

3. It is cyclic. The elements can be created using g^x Where x is an integer from 1 to $\phi(n) = p - 1$.

4.The primitive roots can be thought as the base of logarithm.

Solution to Modular Logarithm Using Discrete Logs

- *Tabulation of Discrete Logarithms*
- *To solve problem of type y=a ^{x} mod n when y is given and x need to be found*

Table 9.6 *Discrete logarithm for* $\mathbf{G} = \langle \mathbf{Z}_7{}^*, \times \rangle$

y	1	2	3	4	5	6
$x = L_3\, y$	6	2	1	4	5	3
$x = L_5\, y$	6	4	5	2	1	3

1.There are 6 elements in this group:1, 2,3, 4, 5, and 6.
2.Find primitive roots

Work at home

- Find x in each of the following cases:

a. $4 \equiv 3^x \pmod 7$.

b. $6 \equiv 5^x \pmod 7$.

Exponentiation: $y = a^x$ $\rightarrow$ **Logarithm:** $x = \log_a y$

Public Key Cryptography

Cryptography and Network Security
by William Stallings

Private-Key Cryptography

- traditional **private/secret/single key** cryptography uses **one** key
- shared by both sender and receiver
- if this key is disclosed communications are compromised
- also is **symmetric**, parties are equal
- hence does not protect sender from receiver forging a message & claiming is sent by sender

Public-Key Cryptography

- probably most significant advance in the 3000 year history of cryptography
- uses **two** keys – a public & a private key
- **asymmetric** since parties are **not** equal
- uses clever application of number theoretic concepts to function
- complements **rather than** replaces private key cryptography

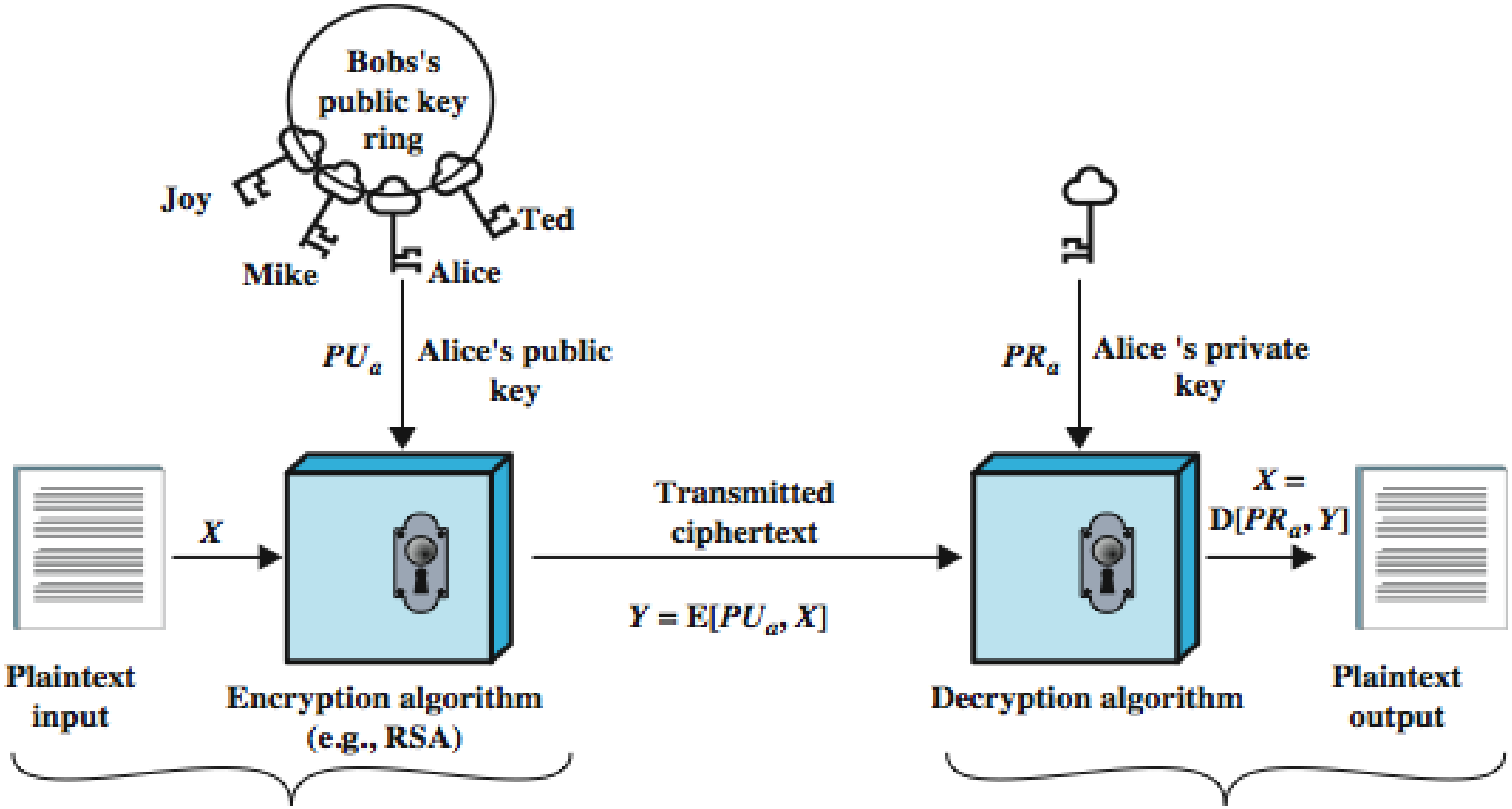
Why Public-Key Cryptography?

- developed to address two key issues:
  - **key distribution** – how to have secure communications in general without having to trust a KDC with your key
  - **digital signatures** – how to verify a message comes intact from the claimed sender
- public invention due to Whitfield Diffie & Martin Hellman at Stanford University in 1976

Public-Key Cryptography

- **public-key/two-key/asymmetric** cryptography involves the use of **two** keys:
  - a **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
  - a related **private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures**
- **infeasible to determine private key from public**
- is **asymmetric** because
  - those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures

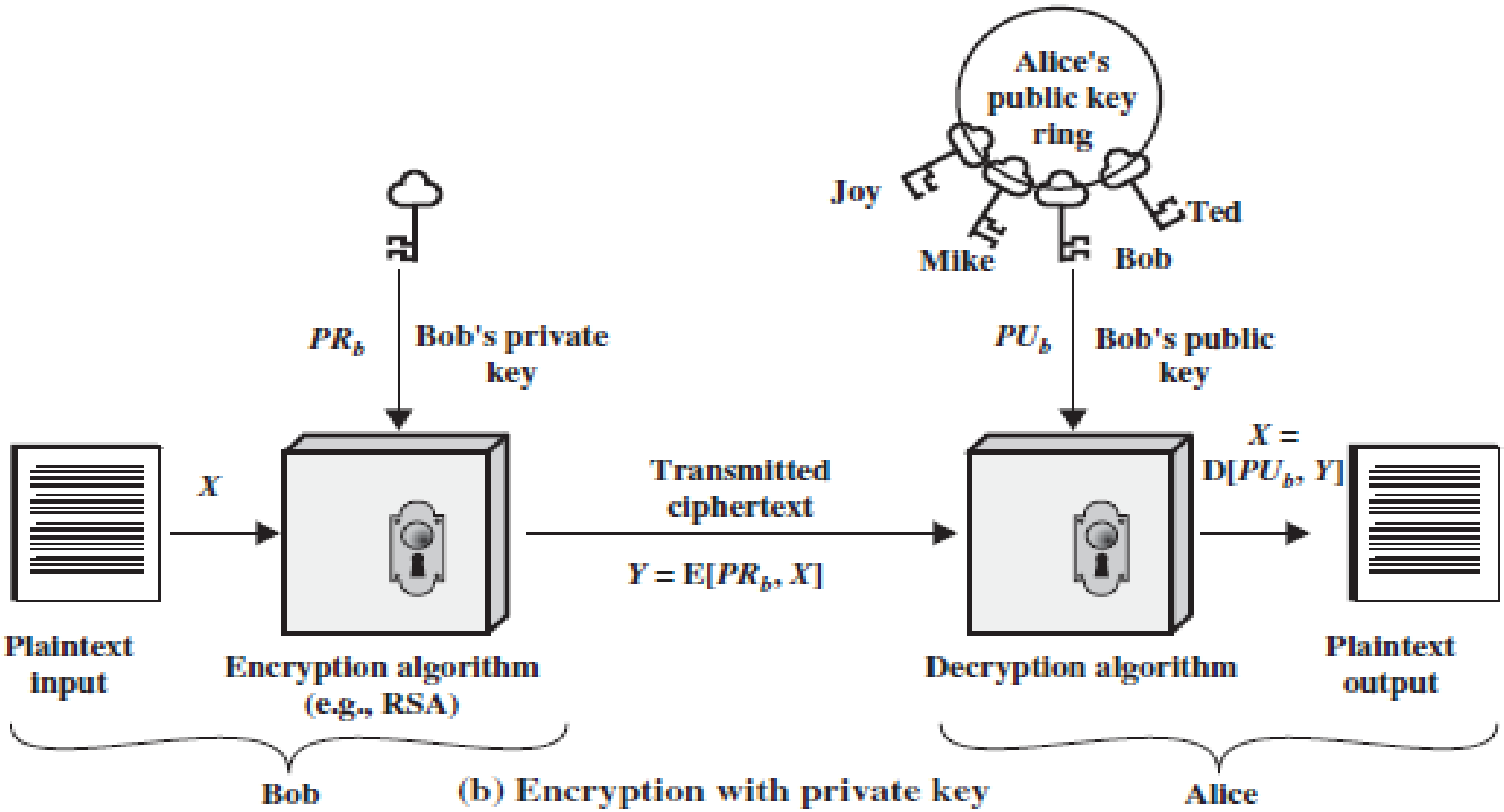
Public-Key Cryptography



(a) Encryption with public key

Bob sends a confidential message to Alice

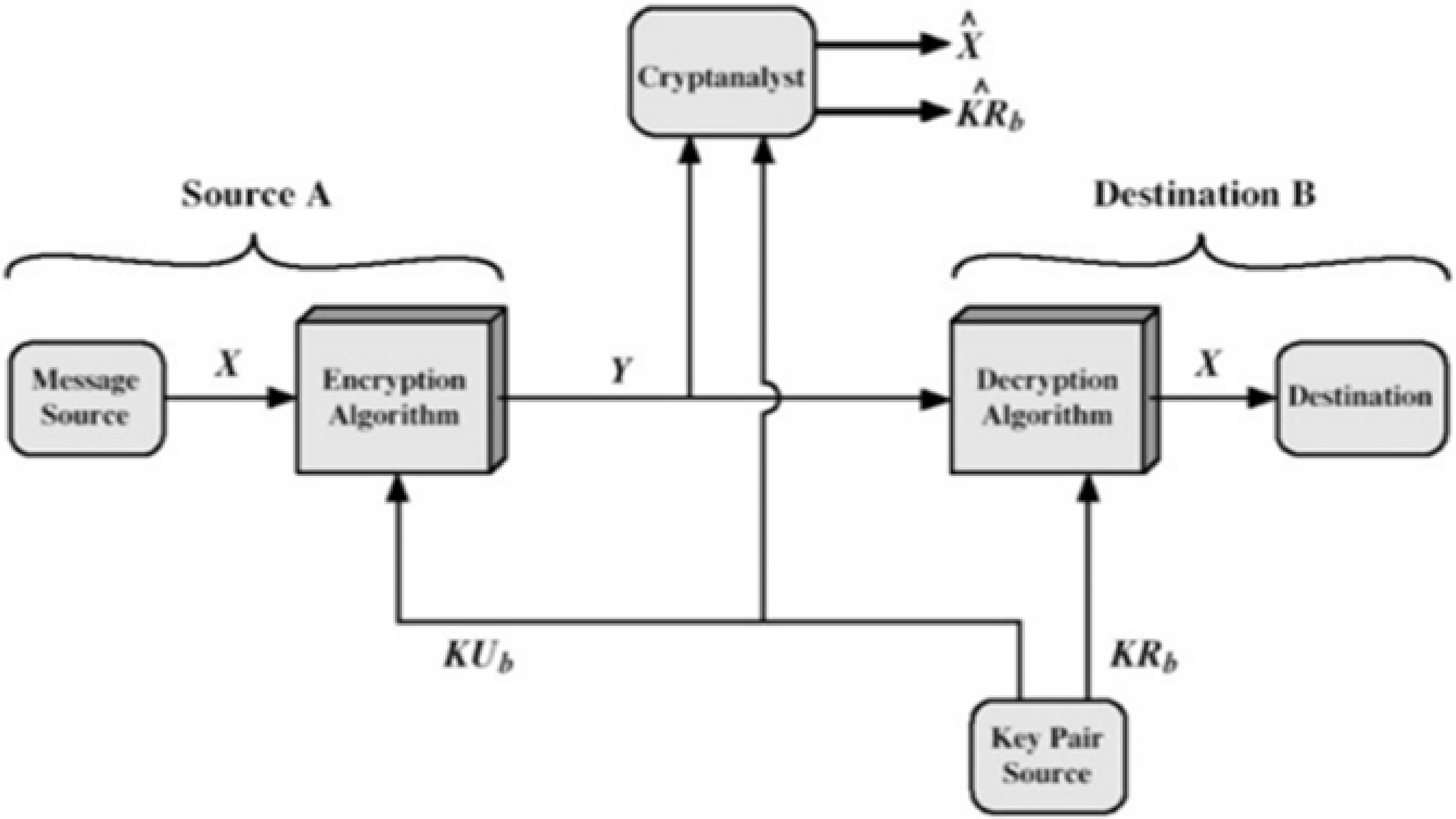
Public-Key Cryptography



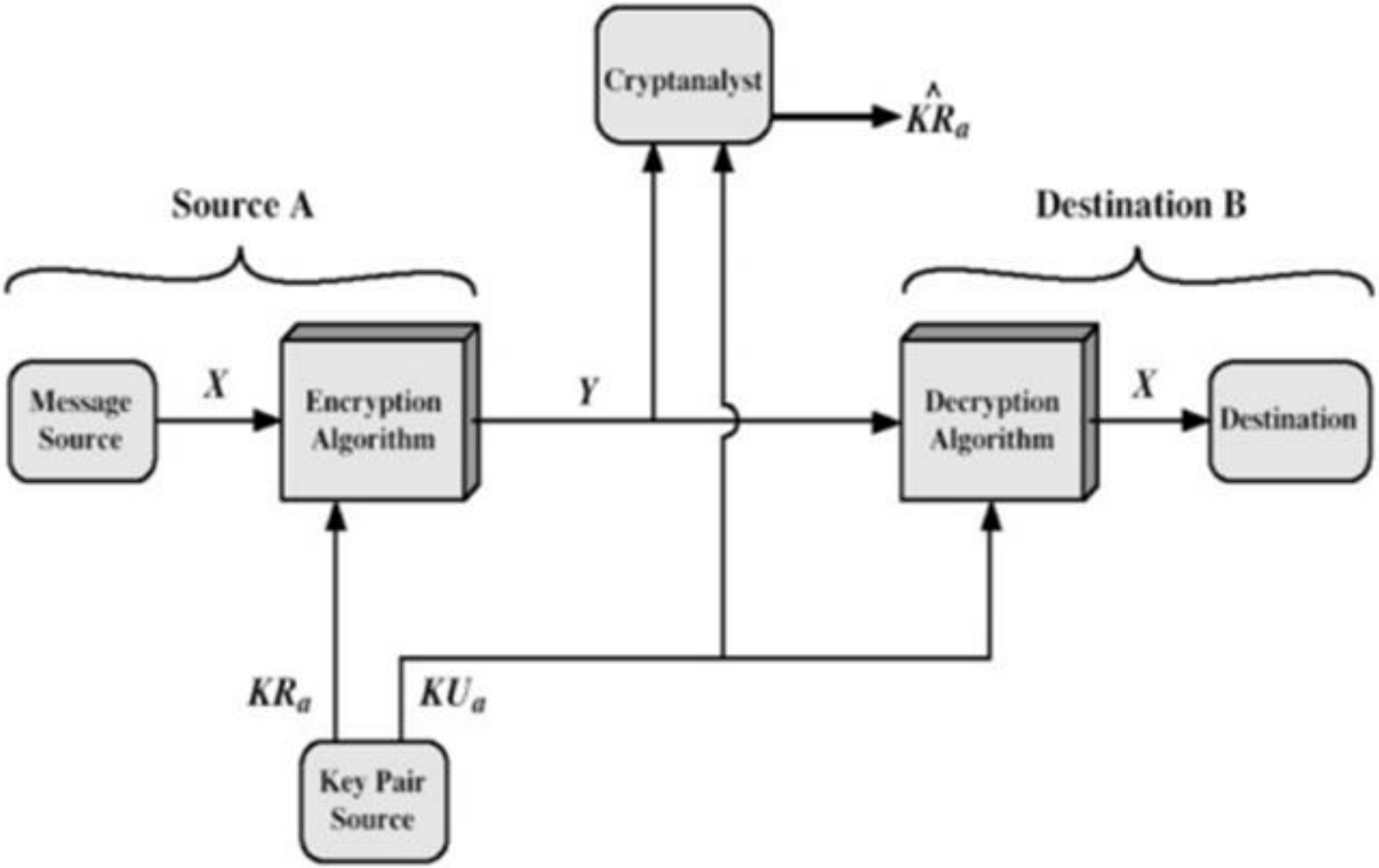
Authentication is achieved here

Symmetric vs Public-Key

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

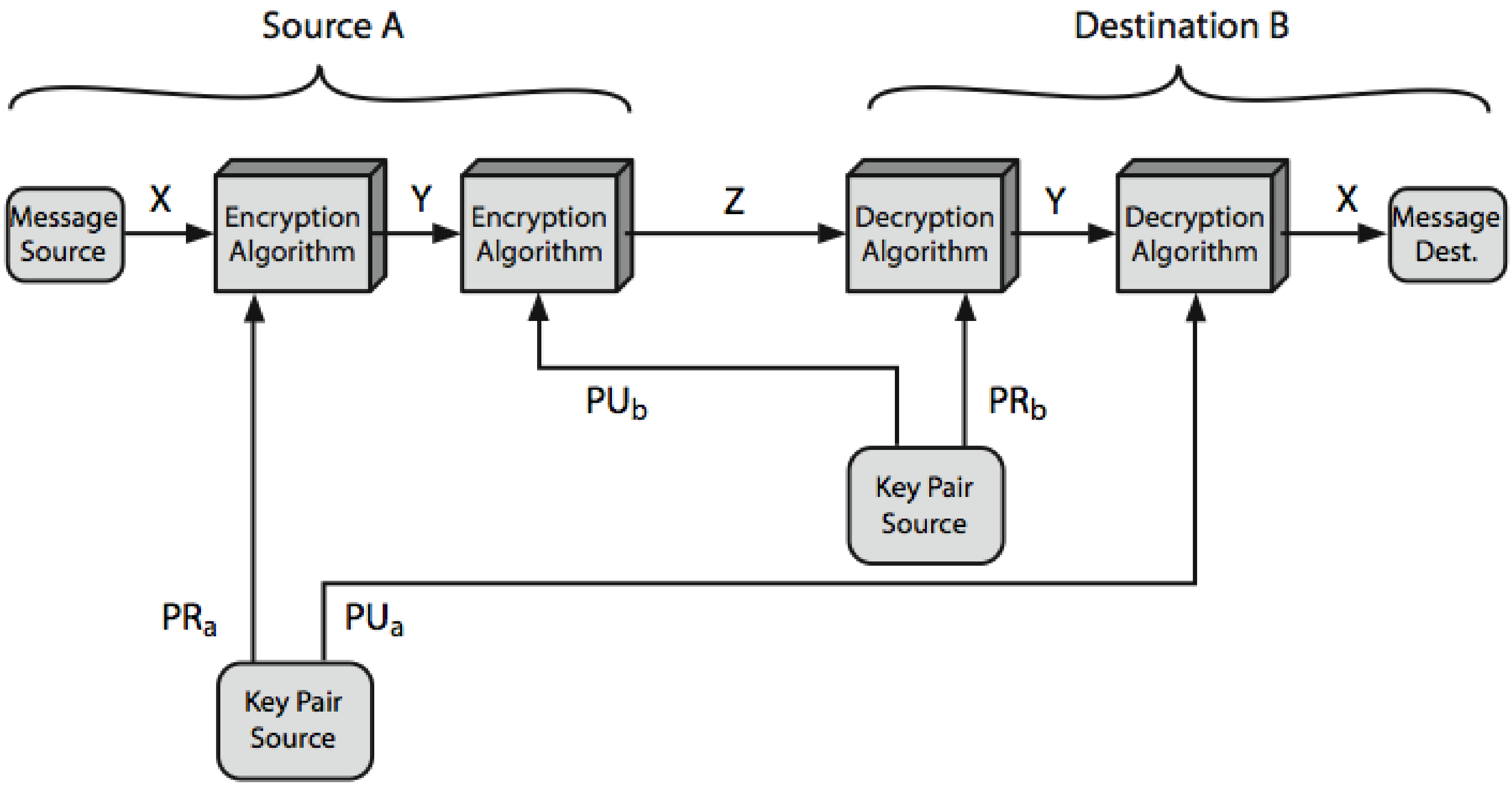


Public-Key Cryptosystem:Secrecy



Public key encryption to provide authentication

Public-Key Cryptosystems



Confidentiality and Authentication

$$Z = \mathrm{E}(PU_b, \mathrm{E}(PR_a, X))$$

$$X = \mathrm{D}(PU_a, \mathrm{D}(PR_b, Z))$$

- Encrypt the message using senders private key. Provides digital signature (authentication).
- Encrypt again using receivers public key. The message can be decrypted by only by the intended receiver (confidentiality).

Public-Key Applications

- can classify uses into 3 categories:
  - **encryption/decryption** (provide secrecy)
  - **digital signatures** (provide authentication)
  - **key exchange** (of session keys)
- some algorithms are suitable for all uses, others are specific to one

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

Public-Key Requirements-Deffie and Hellman

1. It is computationally easy for party B to generate a key pair (public (PU) and private (PR)).
2. It is computationally easy for sender A knowing PUb and the message to be encrypted to generate the corresponding ciphertext C = E(PUb (M)).

- 3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using his private key (PRb) to recover the original message. M = DPRb (C) = DPRb [E(PUb (M))].
- 4. It is computationally infeasible for an opponent, knowing the public key PUb, to determine the private key PRb

5. It is computationally infeasible for an opponent, knowing PUb and C to recover the plaintext message M.

6. A sixth requirement that, although useful, is not necessary for all public-key applications - the encryption and decryption can be applied in either order: M = EPUb [D(PRb (M))] = DPUb [E(PRb (M))].

These are formidable requirements which only a few algorithms have satisfied

Public-Key Requirements

- need a trapdoor one-way function
- one-way function(A one-way function is a function that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy whereas the calculation of the inverse is infeasible: has
  - $Y = f(X)$ easy
  - $X = f^{-1}(Y)$ infeasible

- a trap-door one-way function has
  - $Y = f_k(X)$ easy, if k and X are known
  - $X = f_k^{-1}(Y)$ easy, if k and Y are known
  - $X = f_k^{-1}(Y)$ infeasible, if Y known but k not known
- a practical public-key scheme depends on a suitable trap-door one-way function
- A trap door function is a family of invertible functions f_k

Security of Public Key Schemes-Cryptanalysis

- like private key schemes brute force **exhaustive search** attack is always theoretically possible
- but keys used are too large (>512bits)
- security relies on a **large enough** difference in difficulty between **easy** (en/decrypt) and **hard** (cryptanalyse) problems

- more generally the **hard** problem is known, but is made hard enough to be impractical to break
- requires the use of **very large numbers**
- hence is **slow** compared to private key schemes

Asymmetric Key Algorithm
RSA Algorithm

Ref:Cryptography and Network Security-Atul Kahate

RSA Algorithm

- Ron Rivest , Adi Shamir and Len Adleman at MIT developed the asymmetric key cryptography system.
- RSA solves the problem of key agreements and distribution.
- In this approach each communicating party possesses a key pair, made up of one public key and one private key.
- RSA is the most popular asymmetric key cryptographic algorithm that employ prime numbers.

Data Encryption Standard (RSA)

RSA Pseudo code:

- Select P,Q where P and Q are prime numbers, $P \neq Q$
- Calculate n, where $n = P * Q$
- Calculate Φ (n), where $\Phi(n) = (P-1)(Q-1)$
- Select Random **'e'** such as : $\gcd(\Phi(n), e) = 1$ and $1 < e < \Phi(n)$,
- Calculate **'d'** , where $d.e \equiv 1 \pmod{\varphi(n)}$
- Public key {e,n}
- private key {d,n}

Example 1

Use RSA algorithm to encrypt the following text number: Plaintext: 88

- Select P = 17, Q = 11
- Calculate n , n= P * Q =17 *11 = 187
- Calculate Φ (n),Φ (n) = (P-1)(Q-1)=16 * 10 = 160
- Select Random E such as: gcd (e, Φ (n),) = 1 and 1<e< Φ (n),

  e = 7 because gcd (7,160) = 1
- Calculate d , where d.e ≡ 1 (mod φ(n))

  d * 7 ≡ 1 mod 160 [d = 7^{-1} mod 160]

  d = 23

Cont…

- Public key { 187, 7} {n,e}
- Private key {187, 23} {n,d}

Encryption: $c = m^e \bmod n$

$88^7 \bmod 187 = 11 = \text{Cipher}$

Decryption: $m = c^d \bmod n$

$11^{23} \bmod 187 = 88$

Try this as home work

1. Select primes p=11, q=3 and find out the public and private key. Perform encryption and decryption on the message m=7

2. Consider an RSA cryptosystem with n=pq, where p=7 and q=13. Let the public key be (n,35) and private key $(\varphi(n), p, q, a)$. Then the decrypted value of 10 is ______

Diffie Hellman key exchange

Ref:Cryptography and Network Security- Atul Kahate

Diffie Hellman key exchange

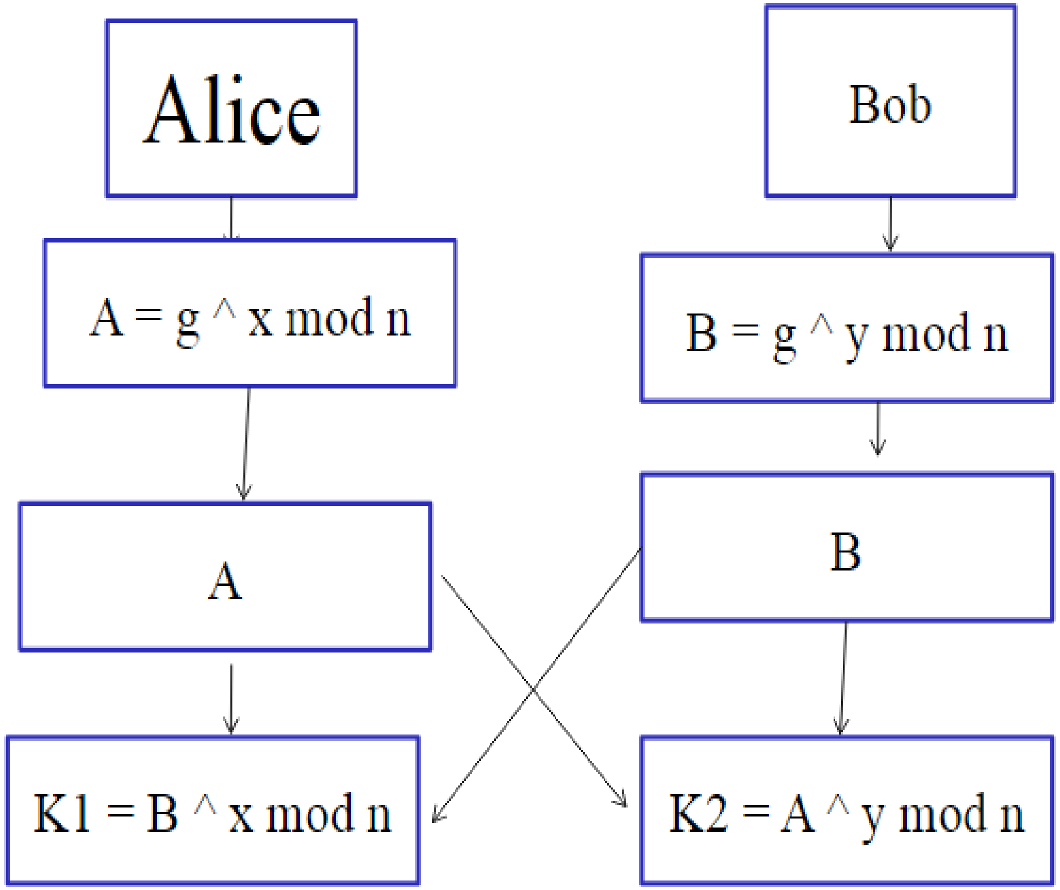
- Devised by Whitefield Diffie and Mertin Hellman as a solution to the problem of key agreement.
- This permits parties for key exchange but not for encryption/Decryption of messages.
- In this technique both the parties interested to communicate can agree on a symmetric key.

Working of the algorithm

Alice and Bob agree on two large prime numbers **'n'** and **'g'**, need not be kept secret.

x,y – random numbers

K1=K2=K that becomes the shared secret key between Alice and Bob



DR MAHALINGAM MCET COLLEGE OF ENGINEERING AND TECHNOLOGY Enlightening Technical Minds

NIA EDUCATIONAL INSTITUTIONS Enlightening Minds

Example

1. Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.

   Let $n = 11$, $g = 7$.

2. Alice chooses another large random number x, and calculates A such that:
   $A = g^x \bmod n$

   Let $x = 3$. Then, we have, $A = 7^3 \bmod 11 = 343 \bmod 11 = 2$.

3. Alice sends the number A to Bob.

   Alice sends 2 to Bob.

4. Bob independently chooses another large random integer y and calculates B such that
   $B = g^y \bmod n$

   Let $y = 6$. Then, we have, $B = 7^6 \bmod 11 = 117649 \bmod 11 = 4$.

5. Bob sends the number B to Alice.

Bob sends 4 to Alice.

6. A now computes the secret key $K1$ as follows:
$K1 = B^x \bmod n$

We have, $K1 = 4^3 \bmod 11 = 64 \bmod 11 = 9.$

7. B now computes the secret key $K2$ as follows:
$K2 = A^y \bmod n$

We have, $K2 = 2^6 \bmod 11 = 64 \bmod 11 = 9.$

Mathematical theory

$$K1 = B^x \bmod n.$$

$$B = g^y \bmod n.$$

$$K1 = (g^y)^x \bmod \mathrm{n} = g^{yx} \bmod n$$

$$K2 = A^y \bmod n.$$

$$A = g^x \bmod n.$$

$$K2 = (g^x)^y \bmod n = g^{xy} \bmod n$$

$$K^{yx} = K^{xy}$$

Therefore, in this case, we have $K1 = K2 = K$.

Problems with the algorithm

- Man in the middle attack also called as Bucket Brigade attack.
- Makes the actual communicators believe that they are talking to each other but they are actually talking to the man-in-the-middle.

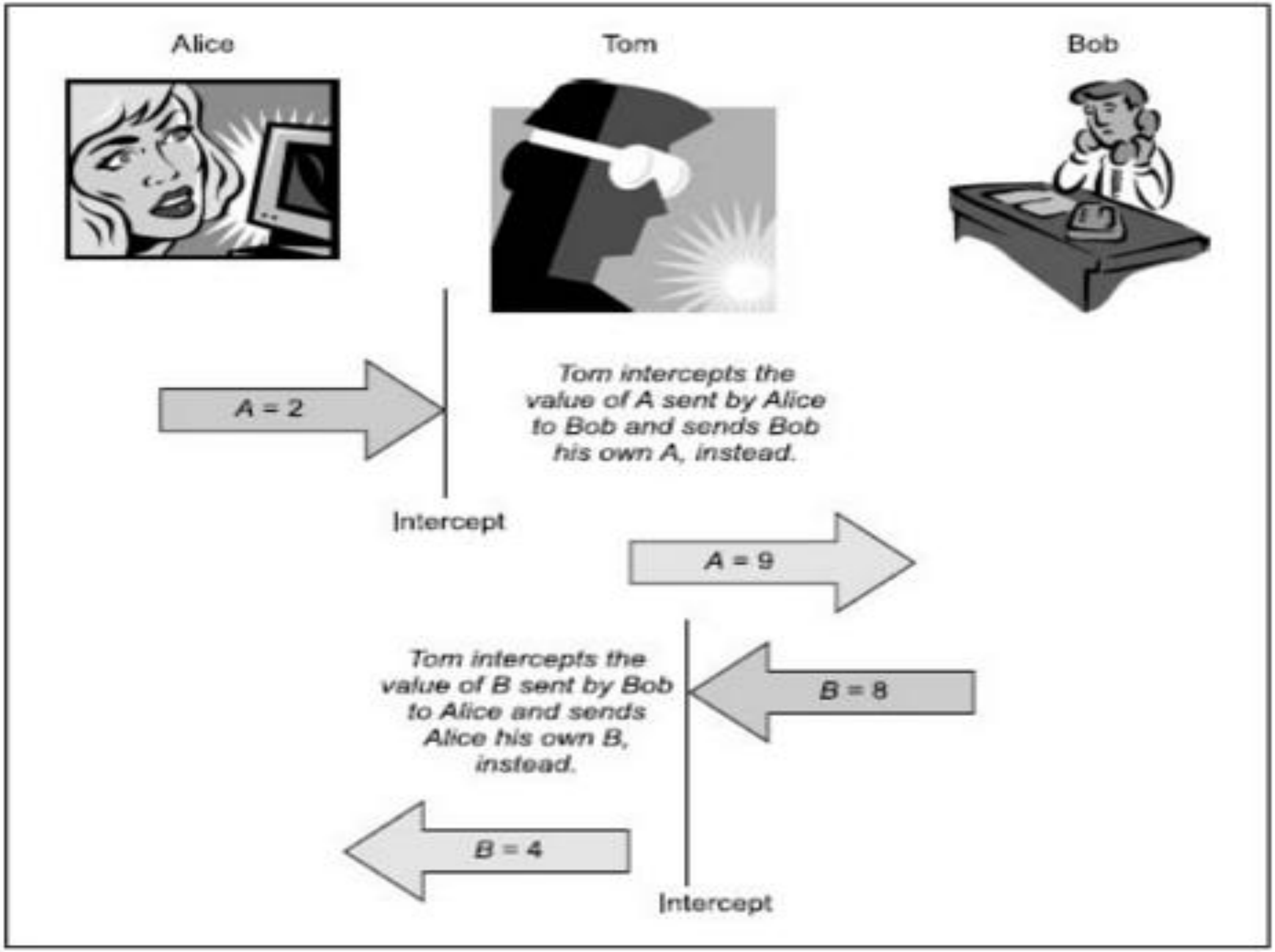
Alice	Tom	Bob
$n = 11, g = 7$	$n = 11, g = 7$	$n = 11, g = 7$

Alice	Tom	Bob
$x = 3$	$x = 8, y = 6$	$y = 9$

Alice	Tom	Bob
$A = g^x \bmod n$ $= 7^3 \bmod 11$ $= 343 \bmod 11$ $= 2$	$A = g^x \bmod n$ $= 7^8 \bmod 11$ $= 5764801 \bmod 11$ $= 9$	$B = g^y \bmod n$ $= 7^9 \bmod 11$ $= 40353607 \bmod 11$ $= 8$
	$B = g^y \bmod n$ $= 7^6 \bmod 11$ $= 117649 \bmod 11$ $= 4$	

DR MAHALINGAM MCET COLLEGE OF ENGINEERING AND TECHNOLOGY Enlightening Technical Minds

NIA EDUCATIONAL INSTITUTIONS | Enlightening Minds


Alice
Tom
Bob
A = 2
Intercept
Tom intercepts the value of A sent by Alice to Bob and sends Bob his own A, instead.
A = 9
B = 8
Tom intercepts the value of B sent by Bob to Alice and sends Alice his own B, instead.
B = 4
Intercept

Alice	Tom	Bob
$A = 2, B = 4^*$	$A = 2, B = 8$	$A = 9^*, B = 8$

(Note: * indicates that these are the values after Tom hijacked and changed them.)

Alice		Tom		Bob	
$K1$	$= B^x \bmod n$	K1	$= B^x \bmod n$	$K2$	$= A^y \bmod n$
	$= 4^3 \bmod 11$		$= 8^8 \bmod 11$		$= 9^9 \bmod 11$
	$= 64 \bmod 11$		$= 16777216 \bmod 11$		$= 387420489 \bmod 11$
	$= 9$		$= 5$		$= 5$
		K2	$= A^y \bmod n$		
			$= 2^6 \bmod 11$		
			$= 64 \bmod 11$		
			$= 9$		

Example:Try it

- Calculate the Diffie hellman key for the public values n=10 and g=3

  Consider x=5 ;y=11

- Suppose p(here n) is a prime of around 300 digits, and a(x) and b(y) at least 100 digits each.
- Discovering the shared secret given g, p,

  g^a mod p and g^b mod p would take longer than the lifetime of the universe, using the best known algorithm. This is called the discrete logarithm problem.

How can two parties agree on a secret value when all of their messages might be overheard by an eavesdropper?

- The Diffie-Hellman algorithm accomplishes this, and is still widely used.
- With sufficiently large inputs, Diffie-Hellman is very secure.