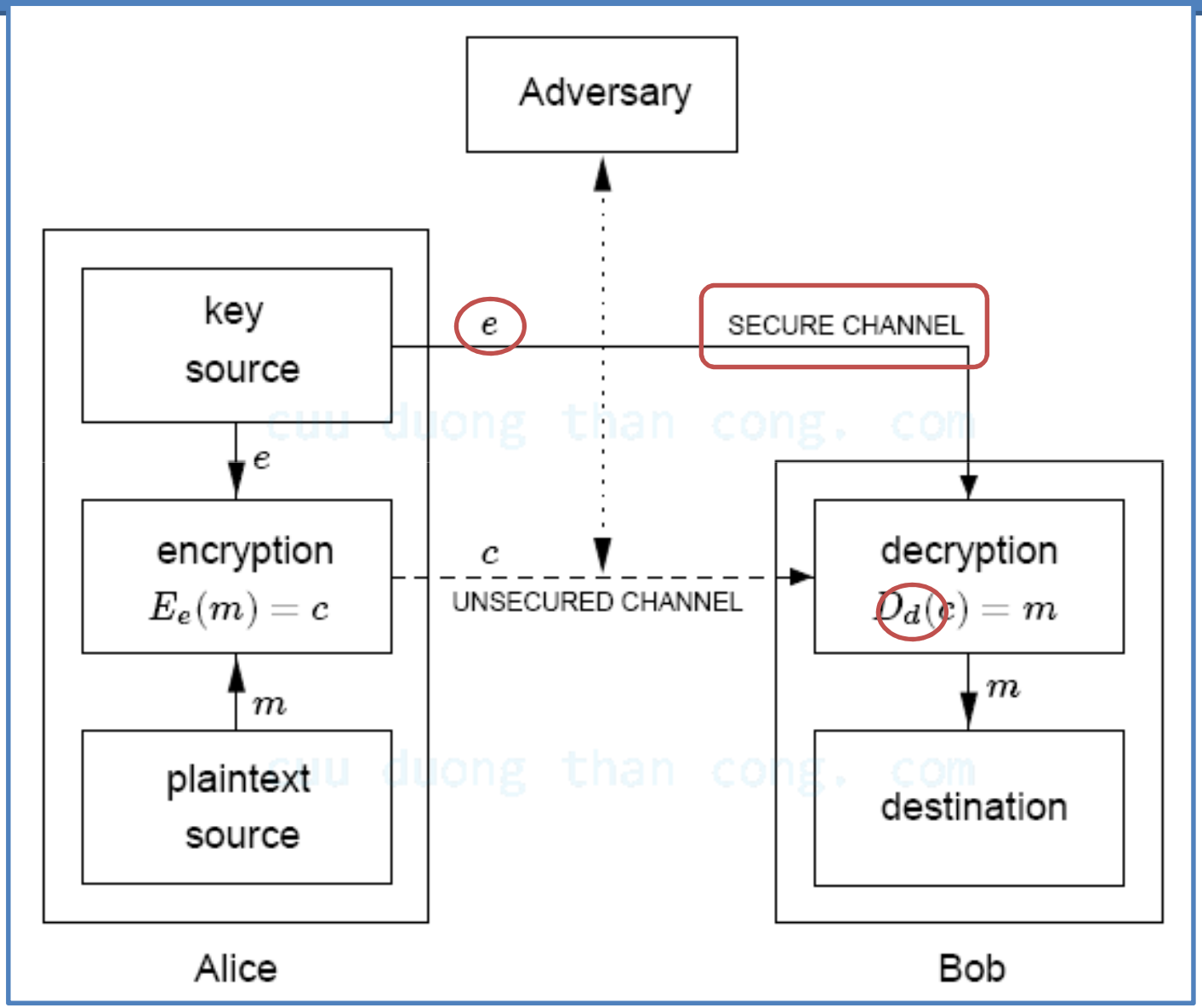
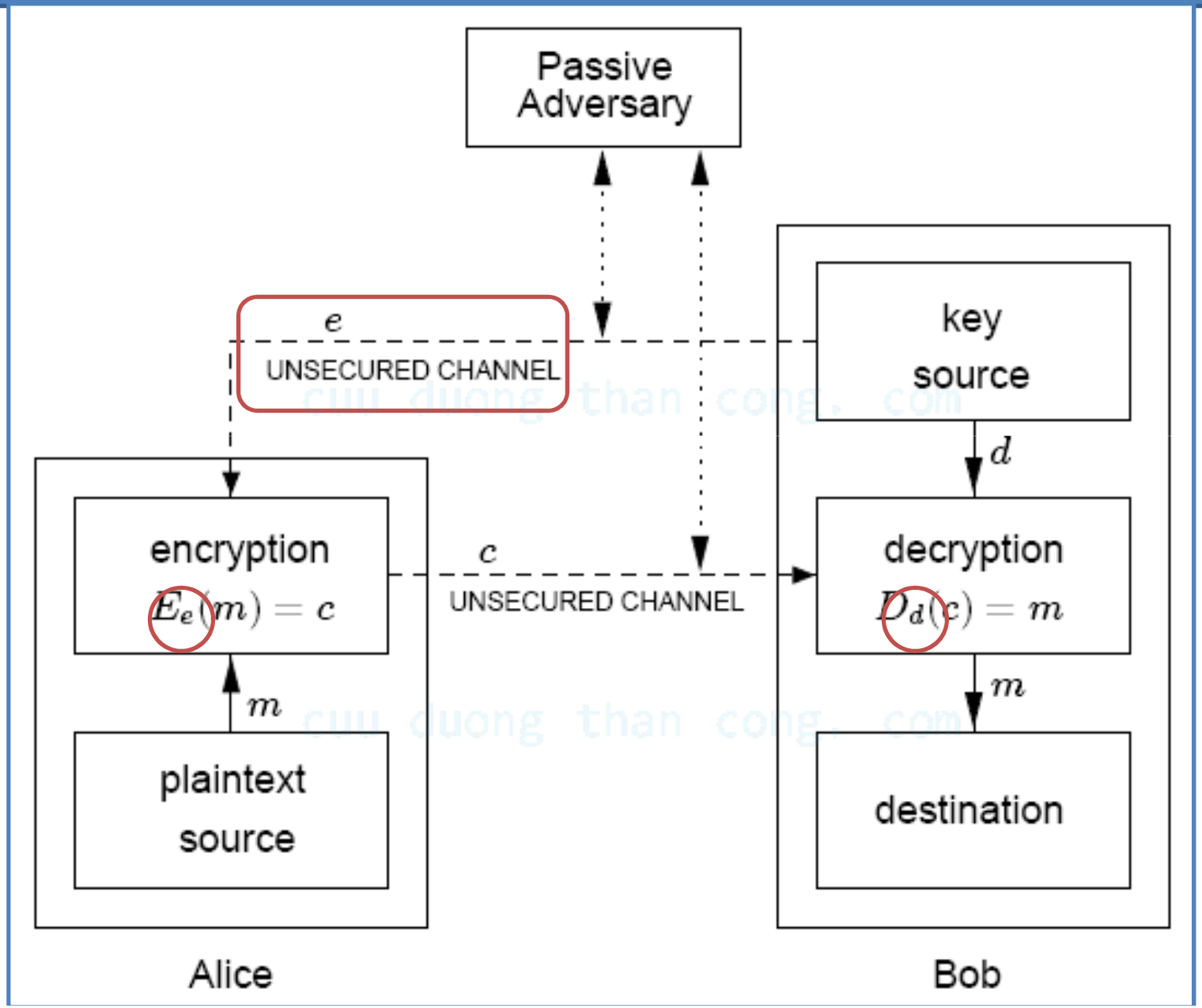
The RSA Cryptosystem

Symmetric key cryptosystem



Public key cryptosystem (PKC)



One-way function

Definition A function f from a set X to a set Y is called a *one-way function* if $f(x)$ is "easy" to compute for all $x \in X$ but for "essentially all" elements $y \in \mathrm{Im}(f)$ it is "computationally infeasible" to find any $x \in X$ such that $f(x) = y$.

Example (*one-way function*) Take $X = \{1, 2, 3, \ldots, 16\}$ and define $f(x) = r_x$ for all $x \in X$ where r_x is the remainder when 3^x is divided by 17. Explicitly,

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Definition A *trapdoor one-way function* is a one-way function $f : X \longrightarrow Y$ with the additional property that given some extra information (called the *trapdoor information*) it becomes feasible to find for any given $y \in \mathrm{Im}(f)$, an $x \in X$ such that $f(x) = y$.

More number Theory

$\mathbb{Z}_n^*$ is a multiplicative group of order $\phi(n)$.

Algorithm 5.1: EUCLIDEAN ALGORITHM(a, b)

$r_0 \leftarrow a$
$r_1 \leftarrow b$
$m \leftarrow 1$
while $r_m \neq 0$
do $\begin{cases} q_m \leftarrow \lfloor \frac{r_{m-1}}{r_m} \rfloor \\ r_{m+1} \leftarrow r_{m-1} - q_m r_m \\ m \leftarrow m + 1 \end{cases}$
$m \leftarrow m - 1$
return $(q_1, \ldots, q_m; r_m)$
comment: $r_m = \gcd(a, b)$

MAPLE command:
igcd(a,b)

example

Exercise

5.1 In Algorithm 5.1, prove that

$$\gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{m-1}, r_m) = r_m$$

and, hence, $r_m = \gcd(a, b)$.

Algorithm 5.2: EXTENDED EUCLIDEAN ALGORITHM(a, b)

$a_0 \leftarrow a$
$b_0 \leftarrow b$
$t_0 \leftarrow 0$
$t \leftarrow 1$
$s_0 \leftarrow 1$
$s \leftarrow 0$
$q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$
$r \leftarrow a_0 - qb_0$

while $r > 0$
do
$temp \leftarrow t_0 - qt$
$t_0 \leftarrow t$
$t \leftarrow temp$
$temp \leftarrow s_0 - qs$
$s_0 \leftarrow s$
$s \leftarrow temp$
$a_0 \leftarrow b_0$
$b_0 \leftarrow r$
$q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$
$r \leftarrow a_0 - qb_0$
$r \leftarrow b_0$
return (r, s, t)
comment: $r = \gcd(a, b)$ and $sa + tb = r$

MAPLE command:
igcdex(a, b, 's', 't')

example

Exercise

5.4 Compute $\gcd(57, 93)$, and find integers s and t such that $57s + 93t = \gcd(57, 93)$.

COROLLARY 5.2 *Suppose* $\gcd(r_0, r_1) = 1$. *Then* $r_1^{-1} \bmod r_0 = t_m \bmod r_0$.

- Proof

$$1 = \gcd(r_0, r_1) = s_m r_0 + t_m r_1.$$

Reducing this equation modulo r_0, we obtain

$$t_m r_1 \equiv 1 \pmod{r_0}.$$

Example 5.1 Suppose we wish to calculate $28^{-1} \bmod 75$. Then we compute the following:

i	r_i	q_i	s_i	t_i
0	75		1	0
1	28	2	0	1
2	19	1	1	−2
3	9	2	−1	3
4	1	9	3	−8

Therefore, we have found that

$$3 \times 75 - 8 \times 28 = 1.$$

Applying Corollary 5.2, we see that

$$28^{-1} \bmod 75 = -8 \bmod 75 = 67.$$

Exercise

5.3 Use the EXTENDED EUCLIDEAN ALGORITHM to compute the following multiplicative inverses:

(a) $17^{-1} \bmod 101$

(b) $357^{-1} \bmod 1234$

(c) $3125^{-1} \bmod 9987$.

Algorithm 5.3: MULTIPLICATIVE INVERSE(a, b)

$a_0 \leftarrow a$
$b_0 \leftarrow b$
$t_0 \leftarrow 0$
$t \leftarrow 1$
$q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$
$r \leftarrow a_0 - qb_0$

example

while $r > 0$
do
$temp \leftarrow (t_0 - qt) \bmod a$
$t_0 \leftarrow t$
$t \leftarrow temp$
$a_0 \leftarrow b_0$
$b_0 \leftarrow r$
$q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$
$r \leftarrow a_0 - qb_0$
if $b_0 \neq 1$
then b has no inverse modulo a
else return (t)

MAPLE command:
a^(-1) mod b

THEOREM 5.3 **(Chinese remainder theorem)** *Suppose $m_1, \ldots, m_r$ are pairwise relatively prime positive integers, and suppose $a_1, \ldots, a_r$ are integers. Then the system of r congruences $x \equiv a_i \pmod{m_i}$ $(1 \leq i \leq r)$ has a unique solution modulo $M = m_1 \times \cdots \times m_r$, which is given by*

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M,$$

where $M_i = M/m_i$ and $y_i = M_i^{-1} \bmod m_i$, for $1 \leq i \leq r$.

MAPLE command:

chrem([a_1, …, a_r],[m_1, …, m_r])

For example, if $x \equiv 5 \pmod 7$, $x \equiv 3 \pmod{11}$ and $x \equiv 10 \pmod{13}$, then this formula tells us that

$$\begin{aligned} x &= (715 \times 5 + 364 \times 3 + 924 \times 10) \bmod 1001 \\ &= 13907 \bmod 1001 \\ &= 894. \end{aligned}$$

This can be verified by reducing 894 modulo 7, 11 and 13. □

Exercise

5.6 Solve the following system of congruences:

$$x \equiv 12 \pmod{25}$$

$$x \equiv 9 \pmod{26}$$

$$x \equiv 23 \pmod{27}.$$

5.7 Solve the following system of congruences:

$$13x \equiv 4 \pmod{99}$$

$$15x \equiv 56 \pmod{101}.$$

HINT First use the EXTENDED EUCLIDEAN ALGORITHM, and then apply the Chinese remainder theorem.

The order of group elements

- **Definition**: The *order* of an element g in G is the smallest positive integer m such that $g^m = 1$.
- **Example**: Find the order of 3 and 2 in $\mathbf{Z}_7^*$.
  - $3^1 = 3$; $3^2 = 2$; $3^3 = 6$; $3^4 = 4$; $3^5 = 5$; $\mathbf{3^6 = 1}$ (mod 7).
  - $2^1 = 2$; $2^2 = 4$; $\mathbf{2^3 = 1}$ (mod 7).

THEOREM 5.4 ***(Lagrange)*** *Suppose G is a multiplicative group of order n, and $g \in G$. Then the order of g divides n.*

  - The order of an element g in $\mathbf{Z}_7^*$ must divides 6 {1, 2, 3, 6}.
  - The order of an element g in $\mathbf{Z}_{11}^*$ must divides 10 {1, 2, 5, 10}.

Facts

COROLLARY 5.5 *If* $b \in \mathbb{Z}_n^*$, *then* $b^{\phi(n)} \equiv 1 \pmod{n}$.

COROLLARY 5.6 **(Fermat)** *Suppose* p *is prime and* $b \in \mathbb{Z}_p$. *Then* $b^p \equiv b \pmod{p}$.

THEOREM 5.7 *If* p *is prime, then* $\mathbb{Z}_p^*$ *is a cyclic group.*

Definition: An element having order $p - 1$ modulo p is call a *primitive element* modulo p.

Observe that α is a primitive element modulo p if and only if

$$\{\alpha^i : 0 \leq i \leq p-2\} = \mathbb{Z}_p{}^*.$$

Now, suppose p is prime and α is a primitive element modulo p. Any element $\beta \in \mathbb{Z}_p{}^*$ can be written as $\beta = \alpha^i$, where $0 \leq i \leq p-2$, in a unique way. It is not difficult to prove that the order of $\beta = \alpha^i$ is

$$\frac{p-1}{\gcd(p-1, i)}.$$

THEOREM 5.8 *Suppose that $p > 2$ is prime and $\alpha \in \mathbb{Z}_p{}^*$. Then α is a primitive element modulo p if and only if $\alpha^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all primes q such that $q \mid (p-1)$.*

we can verify that 2 is a primitive element modulo 13:

$$2^0 \bmod 13 = 1$$

$$2^1 \bmod 13 = 2$$

$$2^2 \bmod 13 = 4$$

$$2^3 \bmod 13 = 8$$

$$2^4 \bmod 13 = 3$$

$$2^5 \bmod 13 = 6$$

$$2^6 \bmod 13 = 12$$

$$2^7 \bmod 13 = 11$$

$$2^8 \bmod 13 = 9$$

$$2^9 \bmod 13 = 5$$

$$2^{10} \bmod 13 = 10$$

$$2^{11} \bmod 13 = 7.$$

Exercise

5.8 Use Theorem 5.8 to find the smallest primitive element modulo 97.

The RSA cryptosystem

Short break

Cryptosystem 5.1: *RSA Cryptosystem*

Let $n = pq$, where p and q are primes. Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, and define

$$\mathcal{K} = \{(n, p, q, a, b) : ab \equiv 1 \pmod{\phi(n)}\}.$$

For $K = (n, p, q, a, b)$, define

$$e_K(x) = x^b \bmod n$$

and

$$d_K(y) = y^a \bmod n$$

($x, y \in \mathbb{Z}_n$). The values n and b comprise the public key, and the values p, q and a form the private key.

Let's verify that encryption and decryption are inverse operations. Since

$$ab \equiv 1 \pmod{\phi(n)},$$

we have that

$$ab = t\phi(n) + 1$$

for some integer $t \geq 1$. Suppose that $x \in \mathbb{Z}_n^*$; then we have

$$\begin{aligned}(x^b)^a &\equiv x^{t\phi(n)+1} \pmod{n} \\ &\equiv (x^{\phi(n)})^t x \pmod{n} \\ &\equiv 1^t x \pmod{n} \\ &\equiv x \pmod{n},\end{aligned}$$

Exercise: show that $(x^b)^a = x \pmod{n}$ if x in $Z_n \setminus Z_n^*$.

Example 5.5 Suppose Bob chooses $p = 101$ and $q = 113$. Then $n = 11413$ and $\phi(n) = 100 \times 112 = 11200$. Since $11200 = 2^6 5^2 7$, an integer b can be used as an encryption exponent if and only if b is not divisible by 2, 5 or 7. (In practice, however, Bob will not factor $\phi(n)$. He will verify that $\gcd(\phi(n), b) = 1$ using Algorithm 5.3. If this is the case, then he will compute b^{-1} at the same time.) Suppose Bob chooses $b = 3533$. Then

$$b^{-1} \bmod 11200 = 6597.$$

Hence, Bob's secret decryption exponent is $a = 6597$.

Bob publishes $n = 11413$ and $b = 3533$ in a directory. Now, suppose Alice wants to encrypt the plaintext 9726 to send to Bob. She will compute

$$9726^{3533} \bmod 11413 = 5761$$

and send the ciphertext 5761 over the channel. When Bob receives the ciphertext 5761, he uses his secret decryption exponent to compute

$$5761^{6597} \bmod 11413 = 9726.$$

Cryptool it!

The security of the *RSA Cryptosystem* is based on the belief that the encryption function $e_K(x) = x^b \bmod n$ is a one-way function, so it will be computationally infeasible for an opponent to decrypt a ciphertext. The trapdoor that allows Bob to decrypt a ciphertext is the knowledge of the factorization $n = pq$. Since Bob knows this factorization, he can compute $\phi(n) = (p-1)(q-1)$, and then compute the decryption exponent a using the EXTENDED EUCLIDEAN ALGORITHM. We will say more about the security of the *RSA Cryptosystem* later on.

Algorithm 5.4: RSA PARAMETER GENERATION

1. Generate two large primes, p and q, such that $p \neq q$
2. $n \leftarrow pq$ and $\phi(n) \leftarrow (p-1)(q-1)$
3. Choose a random b $(1 < b < \phi(n))$ such that $\gcd(b, \phi(n)) = 1$
4. $a \leftarrow b^{-1} \bmod \phi(n)$
5. The public key is (n, b) and the private key is (p, q, a).

Algorithm 5.5: SQUARE-AND-MULTIPLY(x, c, n)

$z \leftarrow 1$
for $i \leftarrow \ell - 1$ **downto** 0
do $\begin{cases} z \leftarrow z^2 \bmod n \\ \textbf{if } c_i = 1 \\ \quad \textbf{then } z \leftarrow (z \times x) \bmod n \end{cases}$
return (z)