Applied Number Theory in Cryptography: RSA

I Am Curious

Sebastian Schlesinger

Zalando SE

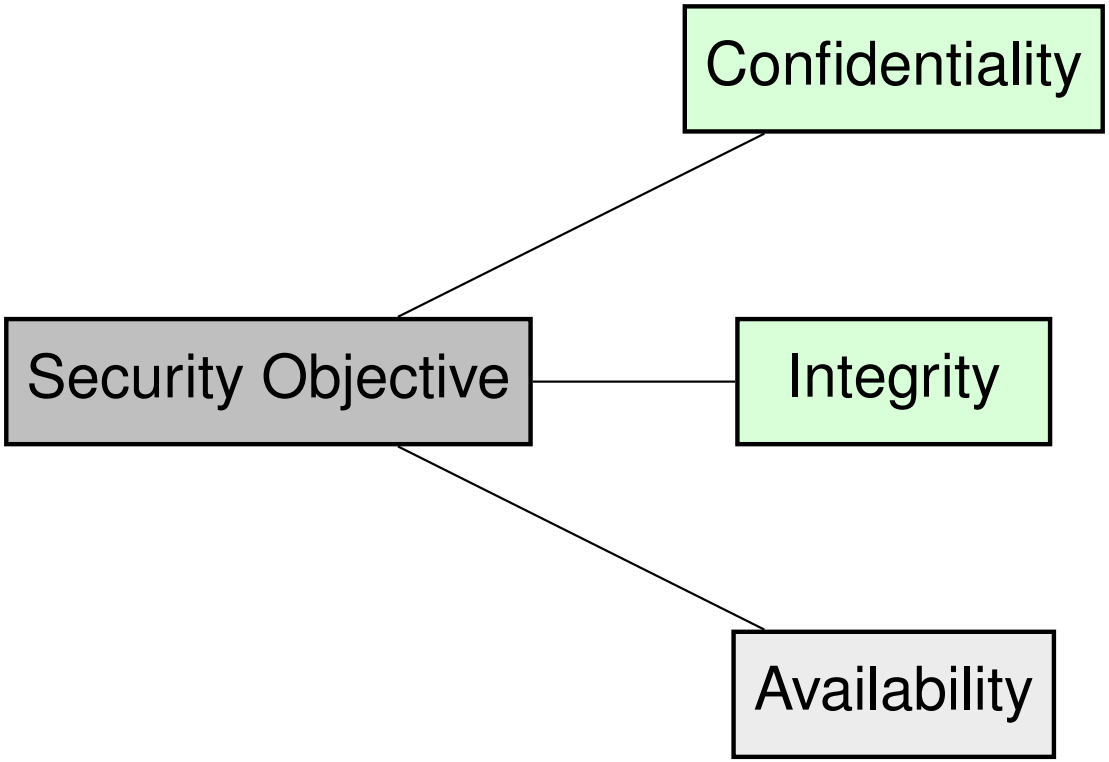
March 5, 2020

Learning objectives of this presentation

- In-depth understanding of RSA with sound mathematical basis
- Ability to assess constraints w.r.t. selection of various parameters in RSA (e.g. key length, set up of encryption key)
- Provide formal foundations for further reading in mathematical cryptography

Outline

Cryptography: Security Objectives



Cryptography Target

No Cryptography Target

The principle of cryptography

Cryptographic System

An encryption is a function $enc : K \times P \to C$ from the cartesian product of the set of keys K and the set of plaintexts P to the set cyphertexts C. A decryption is a function $dec : K \times C \to P$. A suitable decryption has a key k' such that

$$\forall k \in K \forall x \in P : dec(k', enc(k, x)) = x$$

Alternative notation for $enc(k, m)$ is $enc_k(m)$.

Desired Properties for Cryptographic Systems

1. $enc_k(m)$ must be efficiently computable
2. $dec_{k'}(m)$ must be efficiently computable
3. *Resilience against known ciphertext attack:* Given $c_1, ..., c_n \in C$, $dec_{k'}(c_i)$ must not be efficiently computable (without knowledge of k')
4. *Resilience against chosen ciphertext attack:* Given $(m_1, c_1), ..., (m_n, c_n)$, $dec_{k'}(c)$ with $c \neq c_i$ should not be efficiently computable

Symmetric and Asymmetric Cryptography

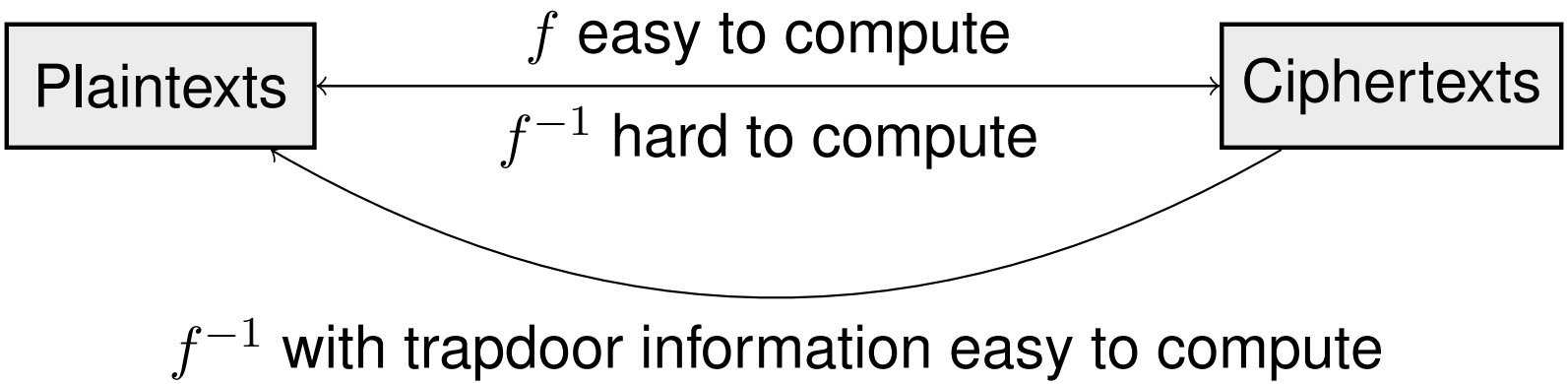
Symmetric and Asymmetric Ciphers

If k' emanates from k efficiently computable, then we speak of a symmetric cipher. Otherwise, it is an asymmetric cipher.

Symmetric and Asymmetric Cryptography

Symmetric and Asymmetric Ciphers

If k' emanates from k efficiently computable, then we speak of a symmetric cipher. Otherwise, it is an asymmetric cipher.



Outline

Now let's start with the math

Groups, Rings, and Fields

Groups

Let $G \neq \emptyset$, $+ : G \times G \to G$ a function. $(G, +)$ is said to be an (Abelian) group if and only if the following properties hold.

Groups, Rings, and Fields

Groups

Let $G \neq \emptyset$, $+ : G \times G \to G$ a function. $(G, +)$ is said to be an (Abelian) group if and only if the following properties hold.

- *Associativity:* $\forall x, y, z \in G : (x + y) + z = x + (y + z)$

Groups, Rings, and Fields

Groups

Let $G \neq \emptyset$, $+ : G \times G \to G$ a function. $(G, +)$ is said to be an (Abelian) group if and only if the following properties hold.

- *Associativity:* $\forall x, y, z \in G : (x + y) + z = x + (y + z)$
- *Commutativity:* $\forall x, y \in G : x + y = y + x$

Groups, Rings, and Fields

Groups

Let $G \neq \emptyset$, $+ : G \times G \to G$ a function. $(G, +)$ is said to be an (Abelian) group if and only if the following properties hold.

- *Associativity:* $\forall x, y, z \in G : (x + y) + z = x + (y + z)$
- *Commutativity:* $\forall x, y \in G : x + y = y + x$
- *Neutral Element:* There exists an alement n such that $\forall x \in G : x + n = x$ (denoted as 0 or 1 for multiplicative groups)

Groups, Rings, and Fields

Groups

Let $G \neq \emptyset$, $+ : G \times G \to G$ a function. $(G, +)$ is said to be an (Abelian) group if and only if the following properties hold.

- *Associativity:* $\forall x, y, z \in G : (x + y) + z = x + (y + z)$
- *Commutativity:* $\forall x, y \in G : x + y = y + x$
- *Neutral Element:* There exists an alement n such that $\forall x \in G : x + n = x$ (denoted as 0 or 1 for multiplicative groups)
- *Inverse Elements:* $\forall x \in G \exists y \in G : x + y = 0$. It is called *inverse* of x, also denoted as $-x$ or x^{-1} if multiplicatively denoted.

Groups, Rings, and Fields

Rings with 1

Let R be a set with at least two neutral elements $0, 1$ w.r.t. the operations $+, \cdot : R \times R \to R$. $(R, +, \cdot)$ is said to be a ring (with 1) if and only if the following properties hold.

Groups, Rings, and Fields

Rings with 1

Let R be a set with at least two neutral elements $0, 1$ w.r.t. the operations $+, \cdot : R \times R \to R$. $(R, +, \cdot)$ is said to be a ring (with 1) if and only if the following properties hold.

- $(R, +)$ is an Abelian group.

Groups, Rings, and Fields

Rings with 1

Let R be a set with at least two neutral elements $0, 1$ w.r.t. the operations $+, \cdot : R \times R \to R$. $(R, +, \cdot)$ is said to be a ring (with 1) if and only if the following properties hold.

- $(R, +)$ is an Abelian group.
- For $(R, \cdot)$ Associativity and Commutativity hold and 1 is the neutral element.

Groups, Rings, and Fields

Rings with 1

Let R be a set with at least two neutral elements $0, 1$ w.r.t. the operations $+, \cdot : R \times R \to R$. $(R, +, \cdot)$ is said to be a ring (with 1) if and only if the following properties hold.

- $(R, +)$ is an Abelian group.
- For $(R, \cdot)$ Associativity and Commutativity hold and 1 is the neutral element.
- *Distributivity:* $\forall x, y, z \in R : (x + y) \cdot z = x \cdot z + y \cdot z$.

Example

An example is the ring of integers $\mathbb{Z}$.

Groups, Rings, and Fields

Fields

Let F be a set with at least two neutral elements $0, 1$ w.r.t. the operations $+, \cdot : F \times F \to F$. $(F, +, \cdot)$ is said to be a field if and only if the following properties hold.

- $(F, +)$ is an Abelian group.
- $(F, \cdot)$ is an Abelian group.
- Distributivity holds.

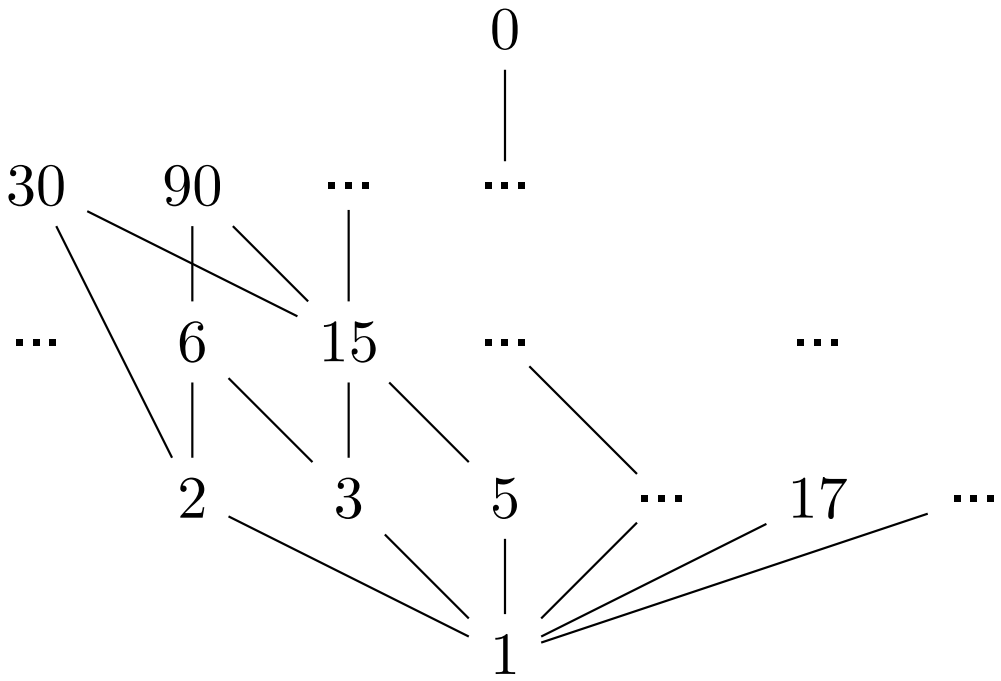
Example

Examples are the rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$.

Important relations on integers

Divisibility Relation

For $a, b \in \mathbb{Z}$ we define the divisibility relation $| \subset \mathbb{Z} \times \mathbb{Z}$ as $a|b :\Leftrightarrow \exists m : a \cdot m = b$. It is an order (reflexive, antisymmetric, transitive).



Important relations on integers

Equivalence mod n

For $a, b, n \in \mathbb{Z}$, we define the relation $\equiv \subset \mathbb{Z} \times \mathbb{Z}$ as $a \equiv b \mod n :\Leftrightarrow n|(a-b)$. It is an equivalence relation (reflexive, symmetric, transitive).

Important relations on integers

Equivalence mod n

For $a, b, n \in \mathbb{Z}$, we define the relation $\equiv \subset \mathbb{Z} \times \mathbb{Z}$ as $a \equiv b \mod n :\Leftrightarrow n|(a-b)$. It is an equivalence relation (reflexive, symmetric, transitive).

An equivalence class for an element $a \in \mathbb{Z}$ is defined as

$$[a] := \{b \in \mathbb{Z} | a \equiv b \mod n\}$$

Important relations on integers

Equivalence mod n

For $a, b, n \in \mathbb{Z}$, we define the relation $\equiv \subset \mathbb{Z} \times \mathbb{Z}$ as $a \equiv b \mod n :\Leftrightarrow n|(a-b)$. It is an equivalence relation (reflexive, symmetric, transitive).

An equivalence class for an element $a \in \mathbb{Z}$ is defined as

$$[a] := \{b \in \mathbb{Z} | a \equiv b \mod n\}$$

Elements in $[a]$ yield all the same residue by dividing through n. Note that

$$\forall x \in \mathbb{Z} \exists \xi, \eta \in \mathbb{Z} : x = \xi \cdot n + \eta \wedge 0 \leq \eta < n$$

and ξ, η are unique.

Factor Ring

Factor Ring

The set of equivalence classes $\mod n$ is defined as

$$\mathbb{Z}/n\mathbb{Z} := \{[a] | a \in \mathbb{Z}\} = \{[0], [1], ..., [n-1]\}$$

Factor Ring

Factor Ring

The set of equivalence classes $\mod n$ is defined as

$$\mathbb{Z}/n\mathbb{Z} := \{[a] | a \in \mathbb{Z}\} = \{[0], [1], ..., [n-1]\}$$

We define operations $+, \cdot$ on it as

$$[a] + [b] := [a + b], [a] \cdot [b] := [a \cdot b]$$

This yields a ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

Subgroups and Lagrange's Theorem

Lagrange's theorem

For a group G, we call $\#G := ord(G)$ the order of G. For a subgroup U of G always $ord(U)|ord(G)$.

Subgroups and Lagrange's Theorem

Lagrange's theorem

For a group G, we call $\#G := ord(G)$ the order of G. For a subgroup U of G always $ord(U)|ord(G)$.

Orders of elements

For an element $g \in G$ in a group G, the set $\{g^k | k \in \mathbb{Z}\}$ is a subgroup of G, its order is denoted $ord(g)$.

Subgroups and Lagrange's Theorem

Lagrange's theorem

For a group G, we call $\#G := ord(G)$ the order of G. For a subgroup U of G always $ord(U)|ord(G)$.

Orders of elements

For an element $g \in G$ in a group G, the set $\{g^k | k \in \mathbb{Z}\}$ is a subgroup of G, its order is denoted $ord(g)$.

Corollary to Lagrange's Theorem

For every element $g \in G$ it holds $g^{ord(G)} = 1$.

Ring's multiplikative subgroups and Euler's phi

Ring's multiplicative subgroup

For a ring R, we denote the set $R^* := \{x \in R | \exists y : x \cdot y = 1\}$, which is a multiplicative subgroup of $(R, \cdot)$.

Ring's multiplikative subgroups and Euler's phi

Ring's multiplicative subgroup

For a ring R, we denote the set $R^* := \{x \in R | \exists y : x \cdot y = 1\}$, which is a multiplicative subgroup of $(R, \cdot)$.

Sufficient condition for $a \in (\mathbb{Z}/n\mathbb{Z})^*$:

$$\gcd(a, n) = 1$$

Ring's multiplikative subgroups and Euler's phi

Ring's multiplicative subgroup

For a ring R, we denote the set $R^* := \{x \in R | \exists y : x \cdot y = 1\}$, which is a multiplicative subgroup of $(R, \cdot)$.

Sufficient condition for $a \in (\mathbb{Z}/n\mathbb{Z})^*$:

$$\gcd(a, n) = 1$$

Examples

$[1], [3] \in (\mathbb{Z}/4\mathbb{Z})^*$:
$[1]^{-1} = [1], [3]^{-1} = 3, [2] \notin (\mathbb{Z}/4\mathbb{Z})^*$ ($[2] \cdot [2] = [0], [2] \cdot [3] = [2]$)
$1, 2, 3, 4 \in (\mathbb{Z}/5\mathbb{Z})^*$

Euler's phi function

Euler's Phi

We define $\varphi(n) := \#\left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

Euler's phi function

Euler's Phi

We define $\varphi(n) := \#\left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

Formula for calculating Euler's phi

For $n = \prod_{p|n} p^{k_p}$, we can calculate

$$\varphi(n) = \prod_{p|n} p^{k_p - 1}(p-1) = \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Euler's phi function

Euler's Phi

We define $\varphi(n) := \#\left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

Formula for calculating Euler's phi

For $n = \prod_{p|n} p^{k_p}$, we can calculate

$$\varphi(n) = \prod_{p|n} p^{k_p - 1}(p-1) = \prod_{p|n}\left(1 - \frac{1}{p}\right)$$

Particularly if $n = p \cdot q$, we have

$$\varphi(n) = (p-1)\cdot(q-1)$$

Outline

Now you no the basics, let's move on to the algorithm...

Encryption

Preparation - the public key

Select two primes p and q and calculate $n = p \cdot q$.

Encryption

Preparation - the public key

Select two primes p and q and calculate $n = p \cdot q$.
Select e with $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.

Encryption

Preparation - the public key

Select two primes p and q and calculate $n = p \cdot q$.
Select e with $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
The pair (n, e) is the public key.

Encryption

Preparation - the public key

Select two primes p and q and calculate $n = p \cdot q$.
Select e with $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
The pair (n, e) is the public key.

For example, $n = 5 \cdot 11 = 55$, $\varphi(n) = 4 \cdot 10 = 40$, $e = 7$.

Encryption

Preparation - the public key

Select two primes p and q and calculate $n = p \cdot q$.
Select e with $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
The pair (n, e) is the public key.

For example, $n = 5 \cdot 11 = 55$, $\varphi(n) = 4 \cdot 10 = 40$, $e = 7$.

Encryption

A message m with $1 < m < n$ is encrypted as follows:

$$m^e \equiv c \mod n$$

Encryption

Preparation - the public key

Select two primes p and q and calculate $n = p \cdot q$.
Select e with $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
The pair (n, e) is the public key.

For example, $n = 5 \cdot 11 = 55$, $\varphi(n) = 4 \cdot 10 = 40$, $e = 7$.

Encryption

A message m with $1 < m < n$ is encrypted as follows:

$$m^e \equiv c \mod n$$

Say, we encrypt $m = 8$. This yields $m^e = 8^7 \equiv 2 \mod 55$, which means 8 is encrypted by 2.

Decryption

Private Key

The private key d fulfills

$$d \cdot e \equiv 1 \mod \varphi(n)$$

d can be obtained via Enhanced Euclidean Algorithm.

Enhanced Euclidean Algorithm

Purpose of the Enhanced Euclidean Algorithm (EEA)

The purpose of the EEA is to obtain a representation of the form

$$\gcd(a, b) = \xi \cdot a + \eta \cdot b$$

Enhanced Euclidean Algorithm

Purpose of the Enhanced Euclidean Algorithm (EEA)

The purpose of the EEA is to obtain a representation of the form

$$\gcd(a, b) = \xi \cdot a + \eta \cdot b$$

In our example $e = 7, \varphi(n) = 40$,

Enhanced Euclidean Algorithm

Purpose of the Enhanced Euclidean Algorithm (EEA)

The purpose of the EEA is to obtain a representation of the form

$$\gcd(a, b) = \xi \cdot a + \eta \cdot b$$

In our example $e = 7, \varphi(n) = 40$, this yields

$$40 = 5 \cdot 7 + 5, 7 = 1 \cdot 5 + 2, 5 = 2 \cdot 2 + 1$$

Enhanced Euclidean Algorithm

Purpose of the Enhanced Euclidean Algorithm (EEA)

The purpose of the EEA is to obtain a representation of the form

$$\gcd(a, b) = \xi \cdot a + \eta \cdot b$$

In our example $e = 7, \varphi(n) = 40$, this yields

$$40 = 5 \cdot 7 + 5, 7 = 1 \cdot 5 + 2, 5 = 2 \cdot 2 + 1$$

That yields in turn

$$\begin{aligned}\gcd(40, 7) = 1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5) = -2 \cdot 7 + 3 \cdot 5 \\ = -2 \cdot 7 + 3 \cdot (40 - 5 \cdot 7) = 3 \cdot 40 - 17 \cdot 7\end{aligned}$$

Enhanced Euclidean Algorithm

Purpose of the Enhanced Euclidean Algorithm (EEA)

The purpose of the EEA is to obtain a representation of the form

$$\gcd(a, b) = \xi \cdot a + \eta \cdot b$$

In our example $e = 7, \varphi(n) = 40$, this yields

$$40 = 5 \cdot 7 + 5, 7 = 1 \cdot 5 + 2, 5 = 2 \cdot 2 + 1$$

That yields in turn

$$\begin{aligned}\gcd(40, 7) = 1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5) = -2 \cdot 7 + 3 \cdot 5 \\ = -2 \cdot 7 + 3 \cdot (40 - 5 \cdot 7) = 3 \cdot 40 - 17 \cdot 7\end{aligned}$$

We were looking for d such that $d \cdot e \equiv 1 \mod \varphi(n)$. This translates in the example to $d = -17 \equiv 23 \mod 40$

Decryption Example

In our example, we have obtained $d = 23$. We had $m = 8$ and obtained $c = 2$. To decrypt, we calculate

$$c^d = 2^{23} \equiv 8 \mod 55$$

Soundness proof: From [complex looking math] it straightforwardly follows...

Soundness for $gcd(m, n) = 1$

If $gcd(m, n) = 1$, then $m \in (\mathbb{Z}/n\mathbb{Z})^*$.

Soundness for $gcd(m, n) = 1$

If $gcd(m, n) = 1$, then $m \in (\mathbb{Z}/n\mathbb{Z})^*$.
We know that $\#\,(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$ and $\forall x \in (\mathbb{Z}/n\mathbb{Z})^* : x^{\varphi(n)} = 1$.

Soundness for $gcd(m, n) = 1$

If $gcd(m, n) = 1$, then $m \in (\mathbb{Z}/n\mathbb{Z})^*$.
We know that $\#\,(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$ and $\forall x \in (\mathbb{Z}/n\mathbb{Z})^* : x^{\varphi(n)} = 1$.
Hence, $c^d = (m^e)^d = m^{e \cdot d} = m^{k \cdot \varphi(n)+1} = m^{k \cdot \varphi(n)} \cdot m = 1 \cdot m = m$

□

Soundness for $gcd(m, n) \neq 1$

Let w.l.o.g. $\gcd(m, n) = p$, i.e., $p|m$.

Soundness for $gcd(m, n) \neq 1$

Let w.l.o.g. $\gcd(m, n) = p$, i.e., $p|m$.
Then $m = p$ or $m = 2p$ or $m = p^2$ etc. However, $\gcd(m, q) = 1$.

Soundness for $gcd(m, n) \neq 1$

Let w.l.o.g. $\gcd(m, n) = p$, i.e., $p|m$.
Then $m = p$ or $m = 2p$ or $m = p^2$ etc. However, $\gcd(m, q) = 1$.
This means $m \in (\mathbb{Z}/q\mathbb{Z})^*$, which in turn yields $m^{q-1} = 1$, and therefore $m^{k\cdot(q-1)+1} \equiv m \mod q$.

Soundness for $gcd(m, n) \neq 1$

Let w.l.o.g. $\gcd(m, n) = p$, i.e., $p|m$.
Then $m = p$ or $m = 2p$ or $m = p^2$ etc. However, $\gcd(m, q) = 1$.
This means $m \in (\mathbb{Z}/q\mathbb{Z})^*$, which in turn yields $m^{q-1} = 1$, and therefore $m^{k\cdot(q-1)+1} \equiv m \mod q$.
Then $m^{k\cdot(q-1)\cdot(p-1)+1} \equiv m \mod q$, i.e., $m^{k\cdot\varphi(n)+1} \equiv m \mod q$, and of course $m^{k\cdot\varphi(n)+1} \equiv 0 \mod q$.

Soundness for $gcd(m, n) \neq 1$

Let w.l.o.g. $\gcd(m, n) = p$, i.e., $p|m$.
Then $m = p$ or $m = 2p$ or $m = p^2$ etc. However, $\gcd(m, q) = 1$.
This means $m \in (\mathbb{Z}/q\mathbb{Z})^*$, which in turn yields $m^{q-1} = 1$, and therefore $m^{k\cdot(q-1)+1} \equiv m \mod q$.
Then $m^{k\cdot(q-1)\cdot(p-1)+1} \equiv m \mod q$, i.e., $m^{k\cdot\varphi(n)+1} \equiv m \mod q$, and of course $m^{k\cdot\varphi(n)+1} \equiv 0 \mod q$.
Hence, $m^{k\cdot\varphi(n)+1} - m \equiv 0 \mod q$ and $m^{k\cdot\varphi(n)+1} - m \equiv 0 \mod p$.

Soundness for $gcd(m, n) \neq 1$

Let w.l.o.g. $\gcd(m, n) = p$, i.e., $p|m$.
Then $m = p$ or $m = 2p$ or $m = p^2$ etc. However, $\gcd(m, q) = 1$.
This means $m \in (\mathbb{Z}/q\mathbb{Z})^*$, which in turn yields $m^{q-1} = 1$, and therefore $m^{k\cdot(q-1)+1} \equiv m \mod q$.
Then $m^{k\cdot(q-1)\cdot(p-1)+1} \equiv m \mod q$, i.e., $m^{k\cdot\varphi(n)+1} \equiv m \mod q$, and of course $m^{k\cdot\varphi(n)+1} \equiv 0 \mod q$.
Hence, $m^{k\cdot\varphi(n)+1} - m \equiv 0 \mod q$ and $m^{k\cdot\varphi(n)+1} - m \equiv 0 \mod p$.
Since $\gcd(p, q) = 1$, this yields $m^{k\cdot\varphi(n)+1} - m \equiv 0 \mod p \cdot q$.

□

Are you still with me?

Outline

Issues with chosing p and q

Trivial: If p, q too small.

Issues with chosing p and q

Trivial: If p, q too small.
Another issue: If p, q are too close to $\sqrt{n}$: Fermat factorization

Fermat Factorization

It is based on the formula $x^2 - y^2 = (x + y)(x - y)$.
Particularly we consider $n = pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$.

Issues with chosing p and q

Trivial: If p, q too small.
Another issue: If p, q are too close to $\sqrt{n}$: Fermat factorization

Fermat Factorization

It is based on the formula $x^2 - y^2 = (x + y)(x - y)$.
Particularly we consider $n = pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$.
Let k be the smallest integer so that $k^2 > n$, consider $k^2 - n$
(Note $n = (\sqrt{n})^2$).

Issues with chosing p and q

Trivial: If p, q too small.
Another issue: If p, q are too close to $\sqrt{n}$: Fermat factorization

Fermat Factorization

It is based on the formula $x^2 - y^2 = (x + y)(x - y)$.
Particularly we consider $n = pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$.
Let k be the smallest integer so that $k^2 > n$, consider $k^2 - n$
(Note $n = (\sqrt{n})^2$).
If this is a square, this yields the factorization $n = (k + h)(k - h)$.

Issues with chosing p and q

Trivial: If p, q too small.
Another issue: If p, q are too close to $\sqrt{n}$: Fermat factorization

Fermat Factorization

It is based on the formula $x^2 - y^2 = (x + y)(x - y)$.
Particularly we consider $n = pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$.
Let k be the smallest integer so that $k^2 > n$, consider $k^2 - n$
(Note $n = (\sqrt{n})^2$).
If this is a square, this yields the factorization $n = (k + h)(k - h)$.
If not, try again with $(k + 1)^2 - n$, $(k + 2)^2 - n$ etc.

Example

Let $n = 6699557$, then $\sqrt{n} \approx 2588.35$. Hence, $k = 2589$.

Issues with chosing p and q

Trivial: If p, q too small.
Another issue: If p, q are too close to $\sqrt{n}$: Fermat factorization

Fermat Factorization

It is based on the formula $x^2 - y^2 = (x + y)(x - y)$.
Particularly we consider $n = pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$.
Let k be the smallest integer so that $k^2 > n$, consider $k^2 - n$
(Note $n = (\sqrt{n})^2$).
If this is a square, this yields the factorization $n = (k + h)(k - h)$.
If not, try again with $(k + 1)^2 - n$, $(k + 2)^2 - n$ etc.

Example

Let $n = 6699557$, then $\sqrt{n} \approx 2588.35$. Hence, $k = 2589$.
$k^2 - n = 2589^2 - 6699557 = 58^2$. Hence,
$6699557 = 2589^2 - 58^2 = (2589 + 58)(2589 - 58) = 2647 \cdot 2531$

Small encryption exponent e

Trivial: If $m < n^{1/e}$, then just take $e-$th root of c.

Small encryption exponent e

Trivial: If $m < n^{1/e}$, then just take $e-$th root of c.
If the same message m is sent encrypted with small exponent e, e.g. 3 to different partners (using different moduli n_1, n_2, n_3), then the simultaneous congruence

$$x \equiv c_1 \mod n_1$$

$$x \equiv c_2 \mod n_2$$

$$x \equiv c_3 \mod n_3$$

can be solved by exploiting Chinese remainder theorem.
If $m^3 < n_1 n_2 n_3$, this also implies $x = m^3$, which in turn yields the plaintext m.
Solution: Salting (Add random bit string to message)

Other attacks

- Small decryption exponent d ($d < n^{1/4}$): Attackable if $\gcd(p-1, q-1)$ small. Then d can be calculated.
- Adaptive chosen cypher text attack due to homomorphic property: $(m_1 m_2)^e \equiv m_1^e m_2^e \equiv c_1 c_2 \mod n$.
- Coppersmith attacks: Exploit if messages depend linearly on each other, i.e., $m_1 = a \cdot m_2 + b$
- Cycling attacks: For $c = m^e \mod n$, there is a k such that $c^{e^k} \equiv c \mod n$. Hence, $c^{e^{k-1}} \equiv m \mod n$ (like taking $e-$th root of c). However, proven to be as hard (and therefore as low-likely as factorization)
- Message concealing: If $m^e \equiv m \mod n$ (very small probability).

Thank you for your attention

Any Questions?