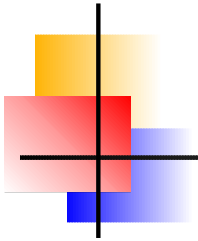
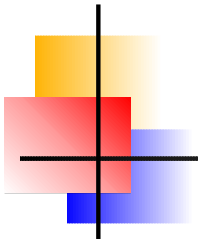


Public Key Cryptography

Stanislav Palúch

Fakulta riadenia a informatiky, Žilinská univerzita

30. novembra 2017



Fundamentals of Number Theory

$\mathbb{N} = \{1, 2, 3, \dots\}$ – the set of **natural** numbers

$\mathbb{Z} = \{0, +1, -1, +2, -2, +3, -3, \dots, \}$ – the set of **integer** numbers

We will say that the integer a **divides** the integer b a write $a|b$, if there exists an integer k such that $b = k.a$.

Remark:
It holds $\forall a \in \mathbb{Z} \;\; 0 = 0.a$. Therefore every integer a divides zero 0 – $a|0$.
0 divides no nonzero integer.

Relation $.|.$ is transitive – if $a|b$ and $b|c$ then $a|c$.
$b = k_1.a$, $c = k_2.b \Rightarrow$ then $c = k_2.b = k_2(k_1.a)) = (k_1.k_2).a$

Let $m \in \mathbb{Z}$. **Trivial divisors of** integer m are the numbers 1, -1, m, $-m$.

Integer $m \in \mathbb{N}$ is called **prime number** if it has only primitive divisors.
Otherwise m is **composite number**.

Fundamental Theorem of Arithmetic

Every natural number $m > 1$ can be uniquely expressed in the form:

$$m = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}, \tag{1}$$

where $p_1 < p_2 < \cdots < p_k$ are mutualy different primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are natural numbers. The problem to express an integer m in the form (1) is called **factorization of the number** m.

Primality testing:
Sieve of Eratosthenes:

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~
~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~
~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~
~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~
~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~
~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~
~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~
~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~

Primality Testing

Other way how to find whether a given number n is prime is based on the fact that if $n = p.q$, where $p > 1$, $q > 1$ and $p \leq q$, then $p \leq \sqrt{n}$.

We have several procedures to find such integer p:

Divide the number n by numbers $2, 3, \ldots, [\sqrt{n}]$.

Or:
Divide the number n by $2, 3$ a then by all number of the form $6k - 1,\ 6k + 1$ less then $\sqrt{n}$.

Or:
Divide the number n by all primes less then $\sqrt{n}$.

The same procedures can be used for factorization of the number n. Factorization resp. primality testing of large numbers is very hard problem. Mentioned methods can not be used for very large numbers. Many advanced sophisticated factorization methods were developed, problems looking as insolvable in near foretime have been solved, but factorization still remains a hard problem.

Greatest Common Divisor

We will say that integer $d \in \mathbb{N}$ is the **gratest common divisor** of numbers $a \in \mathbb{N}$, $b \in \mathbb{N}$ and write $d = GCD(a, b)$, if it holds:

1. $d|a$ and also $d|b$.
2. If $d_1 \neq d$ and $d_1|a$, $d_1|b$, then also $d_1|d$.

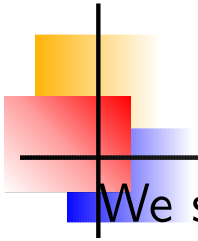
We will say that two integers a, b are **coprime**, if $GCD(a, b) = 1$. Otherwise we will say that the numbers a, b are **commensurable**.

Euclid's algorithm for computing $GCD(a, b)$

Set $r_0 = a$, $r_1 = b$

$$
\begin{aligned}
r_0 &= r_1.q_1 + r_2, && r_2 < r_1 \\
r_1 &= r_2.q_2 + r_3, && r_3 < r_2 \\
&\ldots \\
r_{i-1} &= r_i.q_i + r_{i+1}, && r_{i+1} < r_i \\
&\ldots \\
r_{m-1} &= r_m.q_m + 0
\end{aligned}
$$

$$r_m = GCD(r_0, r_1) = GCD(a, b)$$



Congruence

We say that a and b are **congruent modulo** n and write $a \equiv b \mod n$, if $n|(a-b)$, i.e. if the difference $(a-b)$ is divisible by n.

It holds: Relation $\equiv$ is an equivalence relation on the set of integers $\mathbb{Z}$ (resp. naturals $\mathbb{N}$) – relation $\equiv$ is reflexive, symmetric and transitive.

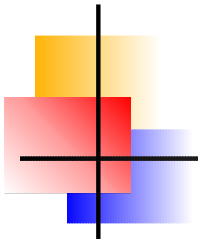
1. $a \equiv a \mod n \; \forall a \in \mathbb{Z}$
2. if $a \equiv b \mod n$ then aj $b \equiv a \mod n$
3. if $a \equiv b \mod n$, $b \equiv c \mod n$, then $a \equiv c \mod n$

$a \equiv b \mod n$ holds if and only if both numbers a, b give the same reminder after integer division by n.

If $a \equiv b \mod n$, then $a * c \equiv b * c \mod n$ for arbitrary integer c.

If $a \equiv b \mod n$, $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$.

If $a * c \equiv b * c \mod n$ and $GCD(c, n) = 1$, then $a \equiv b \mod n$.



Extended Euklid Algorithm

$$
\begin{aligned}
r_0 &= r_1.q_1 + r_2 & t_2 &= (-q_1) \mod r_0 \\
r_1 &= r_2.q_2 + r_3 & t_3 &= (1 - q_2.t_2) \mod r_0 \\
r_2 &= r_3.q_3 + r_4 & t_4 &= (t_2 - q_3.t_3) \mod r_0 \\
&\ldots \\
r_{i-1} &= r_i.q_i + r_{i+1} & t_{i+1} &= (t_{i-1} - q_i.t_i) \mod r_0 \\
r_i &= r_{i+1}.q_{i+1} + r_{i+2} \\
&\ldots \\
r_{m-3} &= r_{m-2}.q_{m-2} + r_{m-1} & t_{m-1} &= (t_{m-3} - q_{m-2}.t_{m-2}) \mod r_0 \\
r_{m-2} &= r_{m-1}.q_{m-1} + r_m & t_m &= (t_{m-2} - q_{m-1}.t_{m-1}) \mod r_0 \\
r_{m-1} &= r_m.q_m + 0 & t_{m+1} &= (t_{m-1} - q_m.t_m) \mod r_0
\end{aligned}
$$

Extended Euklid Algorithm

Proposition: $t_m r_1 \equiv r_m \mod r_0$.
We prove by induction fore $i = 2, 3, \ldots, m$ $t_i r_1 \equiv r_i \mod r_0$.

For $i = 2$:
Since $r_0 = r_1.q_1 + r_2$ it holds $r_2 = r_0 - r_1.q_1$.
Further $t_2 = (-q_1) \mod r_0$ what is equivalent with $q_1 + t_2 \equiv 0 \mod r_0$.
$r_2 - t_2 r_1 \equiv r_0 - r_1 q_1 - t_2 r_1 \equiv r_0 - r_1 \underbrace{(q_1 + t_2)}_{\equiv 0 \mod r_0} \equiv 0 \mod r_0$

For $i = 3$:

$$r_3 - t_3 r_1 \equiv r_1 - r_2 q_2 - t_3 r_1 \equiv r_1 - r_2 q_2 - (1 - q_2 t_2) r_1 \equiv q_2 t_2 r_1 - r_2 q_2 = q_2 \underbrace{(t_2 r_1 - r_2)}_{\equiv 0 \mod r_0} \equiv 0 \mod r_0$$

Suppose that: $t_i r_1 \equiv r_i \mod r_0$, $t_{i-1} r_1 \equiv r_{i-1} \mod r_0$.
Now we will make use of recursive formulas $r_{i+1} = r_{i-1} - r_i q_i$,
$t_{i+1} = t_{i-1} - q_i.t_i$

$$r_{i+1} - t_{i+1} r_1 \equiv r_{i-1} - r_i q_i - (t_{i-1} - q_i.t_i) r_1 \equiv r_{i-1} - r_i q_i - t_{i-1} r_1 + q_i.t_i r_1 \equiv \underbrace{r_{i-1} - t_{i-1} r_1}_{\equiv 0 \mod r_0} + q_i \underbrace{(t_i r_1 - r_i)}_{\equiv 0 \mod r_0} \equiv 0 \mod r_0$$

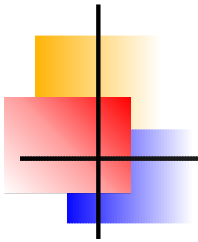
Extended Euklid Algorithm – Program in C

```
#include <stdio.h>
#include <string.h>
int main()
{int a,b,i,nsd,inv,q[100],r[100],t[100];
 printf(" Input a: \n");
 scanf("%d", &a);
 printf(" Input b:\n ");
 scanf("%d", &b);
 for(i=0;i<100;i++) r[i]=0,q[i]=0,t[i]=0;
 i=0; r[0]=a, r[1]=b, t[0]=0, t[1]=1;

 while (r[i+1]!=0)
    {q[i+1]=r[i]/r[i+1];
     r[i+2]=r[i]%r[i+1];
     t[i+2]=(t[i]-q[i+1]*t[i+1])%a;
     if(t[i+2]<0)t[i+2]=t[i+2]+a;
     i++;}

 nsd=r[i], inv=t[i];
 printf("GCD(%d,%d) = %d \n", a, b, nsd);/* GCD(a,b) = nsd*/
 printf("(%d)^ -1 mod %d = %d \n", b, a, inv); /* a^-1 mod b = inv */
 return 0;

}
```



Euler's Totient Function $\phi(n)$

Definition. Let $n \in \mathbb{N}$. Euler's totient function $\phi(n)$ is the number of natural numbers less or equal to n coprime with n.

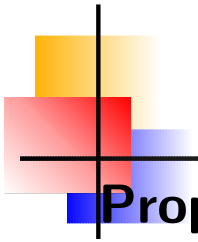
n	1	2	3	4	5	6	7	8	9	10	11	12	13	...
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	...

If p is prime, then all numbers $1, 2, \ldots, p-1$ are coprime with p.

If p is prime, then all numbers comensurable with p less or equal to p^n are $1p, 2p, 3p, \ldots p^{n-1}.p$ – they number is equal to p^{n-1}.

Proposition. Let $p \in \mathbb{N}$ be a prime number, $n \in \mathbb{N}$, $n \geq 1$. Then it holds:

$$\begin{aligned} \phi(p) &= p-1 \\ \phi(p^n) &= p^n - p^{n-1} = p^n\left(1-\frac{1}{p}\right) \end{aligned}$$



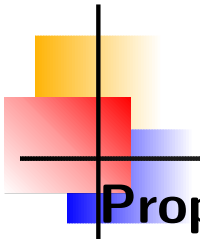
Properties of Euler's Function

Proposition. Leth $a,\ b \in \mathbb{N}$, a, b are coprime. Then

$$\phi(a.b) = \phi(a).\phi(b).$$

Colorary.

$$\phi(n) = \phi(\underbrace{p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}}_{=n}) = \phi(p_1^{\alpha_1}).\phi(p_2^{\alpha_2}).\ldots.\phi(p_k^{\alpha_k}) =$$



Properties of Euler's Function

Proposition. Leth $a,\ b \in \mathbb{N}$, a, b are coprime. Then

$$\phi(a.b) = \phi(a).\phi(b).$$

Colorary.

$$\phi(n) = \phi(\underbrace{p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}}_{=n}) = \phi(p_1^{\alpha_1}).\phi(p_2^{\alpha_2}).\ldots.\phi(p_k^{\alpha_k}) =$$

$$(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}).(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}).\ldots.(p_k^{\alpha_k} - p_k^{\alpha_k - 1}) =$$

Properties of Euler's Function

Proposition. Leth $a,\ b \in \mathbb{N}$, a, b are coprime. Then

$$\phi(a.b) = \phi(a).\phi(b).$$

Colorary.

$$\phi(n) = \phi(\underbrace{p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}}_{=n}) = \phi(p_1^{\alpha_1}).\phi(p_2^{\alpha_2}).\ldots.\phi(p_k^{\alpha_k}) =$$

$$(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}).(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}).\ldots.(p_k^{\alpha_k} - p_k^{\alpha_k - 1}) =$$

$$p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right).p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right).\ldots.p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) =$$

Properties of Euler's Function

Proposition. Leth $a,\ b \in \mathbb{N}$, a, b are coprime. Then

$$\phi(a.b) = \phi(a).\phi(b).$$

Colorary.

$$\phi(n) = \phi(\underbrace{p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}}_{=n}) = \phi(p_1^{\alpha_1}).\phi(p_2^{\alpha_2}).....\phi(p_k^{\alpha_k}) =$$

$$(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}).(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}).....(p_k^{\alpha_k} - p_k^{\alpha_k - 1}) =$$

$$p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right).p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right).....p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) =$$

$$\underbrace{p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}}_{=n}\left(1 - \frac{1}{p_1}\right).\left(1 - \frac{1}{p_2}\right).....\left(1 - \frac{1}{p_k}\right) =$$

Properties of Euler's Function

Proposition. Leth $a,\ b \in \mathbb{N}$, a, b are coprime. Then

$$\phi(a.b) = \phi(a).\phi(b).$$

Colorary.

$$\phi(n) = \phi(\underbrace{p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}}_{=n}) = \phi(p_1^{\alpha_1}).\phi(p_2^{\alpha_2}).....\phi(p_k^{\alpha_k}) =$$

$$(p_1^{\alpha_1} - p_1^{\alpha_1-1}).(p_2^{\alpha_2} - p_2^{\alpha_2-1}).....(p_k^{\alpha_k} - p_k^{\alpha_k-1}) =$$

$$p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right).p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right).....p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) =$$

$$\underbrace{p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}}_{=n}\left(1 - \frac{1}{p_1}\right).\left(1 - \frac{1}{p_2}\right).....\left(1 - \frac{1}{p_k}\right) =$$

$$n.\left(1 - \frac{1}{p_1}\right).\left(1 - \frac{1}{p_2}\right).....\left(1 - \frac{1}{p_k}\right)$$

Especially: For $p,\ q \in \mathbb{N}$ both primes is $\phi(p.q) = (p-1).(q-1)$.

Exponentation $(a+b)^p \equiv a^p + b^p \mod p$

Binomial Theorem:

$$(a+b)^p =$$

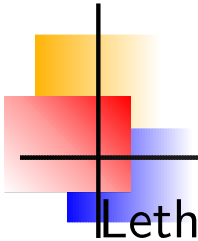
$$a^p + \underbrace{\binom{p}{1} a^{p-1} b^1 + \binom{p}{2} a^{p-2} b^2 + \cdots + \binom{p}{i} a^{p-i} b^i + \cdots + \binom{p}{p-1} a^1 b^{p-1}}_{\text{if } p \text{ is prime, this sum is divisible by } p} + b^p$$

If p is prime, $1 \leq i < p$, then

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{1.2.\ldots.i} = p. \underbrace{\left[\frac{(p-1)\ldots(p-i+1)}{1.2.\ldots.i}\right]}_{\text{this is an integer since } p \text{ can not be divided by ane number of product in de}}$$

Colorary. If is p prime, then

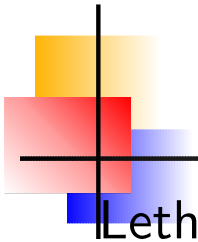
$$(a+b)^p \equiv a^p + b^p \mod p.$$



Fermat's Little Theorem

Leth p be a prime.

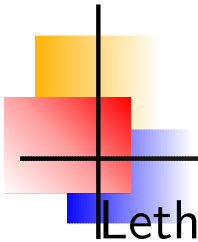
$$2^p \quad = \quad (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p$$



Fermat's Little Theorem

Leth p be a prime.

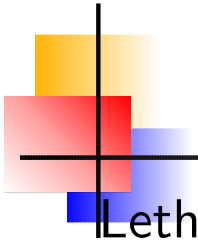
$$\begin{aligned} 2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p \\ 3^p &= (2+1)^p \equiv 2^p + 1^p \equiv 3 \mod p \end{aligned}$$



Fermat's Little Theorem

Leth p be a prime.

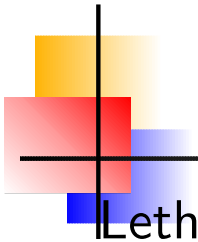
$$
\begin{aligned}
2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p \\
3^p &= (2+1)^p \equiv 2^p + 1^p \equiv 3 \mod p \\
4^p &= (3+1)^p \equiv 3^p + 1^p \equiv 4 \mod p
\end{aligned}
$$



Fermat's Little Theorem

Leth p be a prime.

$$
\begin{aligned}
2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p \\
3^p &= (2+1)^p \equiv 2^p + 1^p \equiv 3 \mod p \\
4^p &= (3+1)^p \equiv 3^p + 1^p \equiv 4 \mod p \\
&\dots \\
c^p &= ((c-1)+1)^p \equiv (c-1)^p + 1^p \equiv (c-1)+1 \equiv c \mod p
\end{aligned}
$$



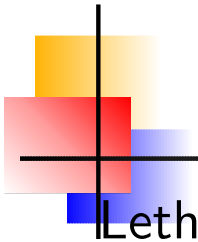
Fermat's Little Theorem

Leth p be a prime.

$$\begin{aligned} 2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p \\ 3^p &= (2+1)^p \equiv 2^p + 1^p \equiv 3 \mod p \\ 4^p &= (3+1)^p \equiv 3^p + 1^p \equiv 4 \mod p \\ &\dots \\ c^p &= ((c-1)+1)^p \equiv (c-1)^p + 1^p \equiv (c-1)+1 \equiv c \mod p \end{aligned}$$

Fermat's little theorem. Let p be a prime number, let c be arbitrary natural number.
Then

$$c^p \equiv c \mod p.$$



Fermat's Little Theorem

Leth p be a prime.

$$\begin{aligned} 2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p \\ 3^p &= (2+1)^p \equiv 2^p + 1^p \equiv 3 \mod p \\ 4^p &= (3+1)^p \equiv 3^p + 1^p \equiv 4 \mod p \\ &\dots \\ c^p &= ((c-1)+1)^p \equiv (c-1)^p + 1^p \equiv (c-1)+1 \equiv c \mod p \end{aligned}$$

Fermat's little theorem. Let p be a prime number, let c be arbitrary natural number.
Then

$$c^p \equiv c \mod p.$$

If moreover $c \in \{1, 2, \dots, p-1\}$, then

$$c^{p-1} \equiv 1 \mod p.$$

Euler's Theorem – a Generalizatin of Fermat's Little Theorem

Let $a_1, a_2, \ldots, a_k$ are all numbers coprime with a number m less than m, where m is arbitrary number, $k = \phi(m)$.
Let x be a number coprime with m and let us study the set of numbers $\{a_1x, a_2x, \ldots, a_kx\}$.
All of those numbers are coprime with m.

It holds $a_ix \not\equiv a_jx \mod m$ for every couple ei, j, $i \neq j$ otherwise it should hold $a_i \equiv a_j \mod m$ (and since$1 \leq a_i,\ a_j \leq m-1$) also $a_i = a_j$.

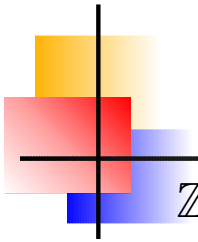
For every a_ix, there exists exactly one $a_{\pi[x]}$ such that $a_ix \equiv a_{\pi[x]} \mod m$.
Therefore it holds:

$$x^{\phi(m)}.\prod_{i=1}^{\phi(m)} a_i \equiv \prod_{i=1}^{\phi(m)} (a_ix) \equiv \prod_{i=1}^{\phi(m)} a_{\pi[i]} \equiv \prod_{i=1}^{\phi(m)} a_i \mod m$$

The product $\prod_{i=1}^{\phi(m)} a_i$ is coprime with m and therefore it is possible to divide both sides of last congruence by this product what results in the following theorem:

Euler's Theorem. It holds for arbitrary number x coprime with the number m

$$x^{\phi(m)} \equiv 1 \mod m.$$



Rings and Fields $\mathbb{Z}_p$

$\mathbb{Z}_p = (\{0, 1, 2, \ldots, p-1\}, \oplus, \otimes)$, where

$$\begin{aligned} a \oplus b &= a + b \mod p \\ a \otimes b &= a.b \mod p \end{aligned}$$

Structure $\mathbb{Z}_p$ is a field if and only if p is a prime number.

Field axioms are:

1. $a \oplus b = b \oplus a$
2. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
3. $a \oplus 0 = 0 \oplus a = a$
4. $\forall a \exists b \ (a \oplus b = b \oplus a = 0)$
5. $a \otimes b = b \otimes a$
6. $(a \otimes b) \otimes c = a \otimes (b \otimes c)$
7. $a \otimes 1 = 1 \otimes a = a$
8. $\forall (a \neq 0) \exists b \ (a \otimes b = b \otimes a = 0)$
9. $a \otimes 0 = 0 \otimes a = 0$
10. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Another Properties of Field Z_p

Let p be a prime.

Let us solve the equation $a \otimes x = 1$, i.e. we are searchig for such x that

$$ax \equiv 1 \mod p.$$

We know that it holds:

$$\begin{aligned} a^{\phi(p)} &\equiv 1 \mod p \\ a.a^{\phi(p)-1} &\equiv 1 \mod p \\ x &\equiv a^{\phi(p)-1} \mod p \\ a^{-1} &\equiv a^{\phi(p)-1} \mod p \end{aligned}$$

Since p is a prime, $\phi(p) = p - 1$, it holds in $\mathbb{Z}_p$:

$$x = a^{-1} = a^{p-2}$$

Equation

$$a \otimes x = b$$

has in $\mathbb{Z}_p$ solution

$$x = a^{-1} \otimes b = a^{p-2} \otimes b.$$

Primality Testing of Large Numbers

Let M be a large number. If M is prime, then Fermat's theorem asserts that for every natural number c, $c < M$ it holds

$$c^{M-1} \equiv 1 \mod M.$$

If we find a natural number $c < M$, such that

$$c^{M-1} \not\equiv 1 \mod M,$$

then M is a composite number.

Fermat's Primality Test.

1. If for some $c < M$ is $c^{M-1} \not\equiv 1 \mod M$, then M is definitely a composite number.
2. If it holds $c^{M-1} \equiv 1 \mod M$ for sufficiently many numbers $c < M$ then M is probably a prime number.

Phill Zimmermann used in PGP the following procedure for finding wheather M is a prime:

- Discarded M if it failed to get through test based on dividing by all 16-bit primes
- Applied Fermat's test for four values of the number c.

Carmichael's Numbers

Carmichael's number – is a composite number M, such that for all $c < M$, c coprime with s M it holds $c^{M-1} \equiv 1 \mod M$.

$$\begin{aligned} 561 &= 3 \cdot 11 \cdot 17 \\ 1105 &= 5 \cdot 13 \cdot 17 \\ 1729 &= 7 \cdot 13 \cdot 19 \\ 2465 &= 5 \cdot 17 \cdot 29 \\ 2821 &= 7 \cdot 13 \cdot 31 \\ 6601 &= 7 \cdot 23 \cdot 41 \\ 8911 &= 7 \cdot 19 \cdot 67 \end{aligned}$$

Properties of a Carmichael's number M:

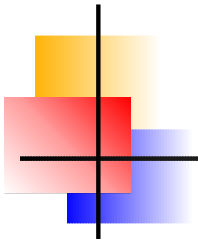
- M is composed from at least 3 primes
- No prime number appears more than once in prime decomposition of M.
- Carmichael's numbers are rare – between 1 and 10^{21} ther is at most 20,138,200 Carmichael's numbers. Probability that a number from interval $\langle 1, 10^{21} \rangle$ is a Carmichael's number is

$$\frac{10^{21}}{2.10^7} = 5.\frac{1}{10^{13}}$$

$$9746347772161 = 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 641$$

$C(N)$ Number of Carmichael numbers between 1 a N

$$N^{0.332} < C(N) < N \cdot \exp\left(- \frac{\ln N \ln \ln \ln N)}{\ln \ln N} \right)$$



RABIN – MILLER Primality Test

1. Express p in the form $p = 1 + 2^s.r$, r odd
2. **For** $i = 1$ **to** t **do**:

   {

   2.1 Choose a random number a such that $2 \leq a \leq p - 2$

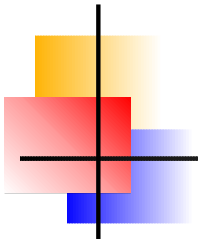
   2.2 Set $y = a^r \mod p$

   2.3 **If** $y \neq 1$ **and** $y \neq p - 1$ **do**:

   ⌈ j=1
   while [$(j \leq s - 1)$ **and** $(y \neq p - 1)$ **]**
   { $y = y^2 \mod p$
   { **If** $y = 1$, **then return** COMPOSITE
   { $j = j + 1$
   ⌊ **If** $y \neq p - 1$, **then return** COMPOSITE

   }

3. **return** PRIME NUMBER WITH PROBABILITY $1 - \left(\frac{1}{4}\right)^t$



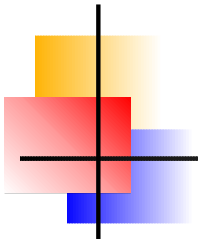
Public Key Cryptography

Disadvantages of symmetric cryptography:

- Every pair of participants has to maintain their key.
- There is a lot of keys, every one has to be kept secret.

Principle of public key cryptography:

- Every participant A has one couple of keys –
  A public key $KV(A)$ and a private key $KT(A)$.
  He publishes his public key $KV(A)$, his private key $KT(A)$ keeps in secret.
- Participant A encipheres a message x to participant B in such a way, that it finds public key $KV(B)$ of participant B and transmits ciphertext $y = E_{KV(B)}(x)$.
- Participant B deciphers ciphertext y using formula $x = D_{KT(B)}(y)$.



RSA algoritmus

1. Participant A chooses two large secret primes p, q.
2. $n = p \cdot q$
3. $\phi(n) = (p-1)(q-1)$
4. Participant A chooses two numbers $0 < e < \phi(n)$, $0 < d < \phi(n)$ such that

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

5. Public key of partipant A is the couple (e, n), his private key is the copule (d, n)
6. Participant B encipheres message $x < n$ for participant A as follows:

$$y = x^e \mod n.$$

7. Participant A decipheres ciphertest y using forumla:

$$x = y^d \mod n.$$

RSA Algorithm – Choosing Primes p, q

Problem how to choose primes p, q.

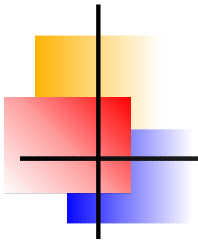
- They must be sufficiently large – at least 1024 bits.
- Primality testing – to use a probability primality test.
- There is enough primes. Number of primes less than n is $\approx \frac{n}{\ln n}$.

Sometimes is required that p, q are so called strong primes.
Prime number p is strong prime, if

1. p is large
2. $p-1$ has a large prime factor, i.e. $p = a_1 p_1 + 1$ for some large prime number p_1.
3. $p_1 - 1$ has a large prime factor, i.e. $p_1 = a_2 p_2 + 1$ for some large prime number p_2.
4. $p+1$ has a large prime factor, i.e. $p = a_3 p_3 + 1$ for some large prime number p_3

Preference of strong primes was motivated by an effort to make some factorization method more difficult. Discovering of next methods of factorization showed that strong primes do not cause for them no additional problem.

Bruce Schneier nor Philip Zimmerman do not recomend strong primes.



RSA Algorithm – Selection of Numbers e, d.

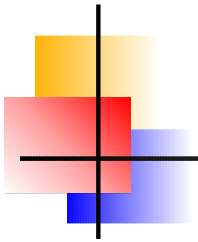
Problem of choosing numbers e, d.

- Very often is used $e = 65537 = 2^{16} + 1$. e is a prime.
- Number d such that $e \cdot d \equiv 1 \mod \phi(n)$ can be calculated by extended Euklid's algorithm.

Exponentation $x^d \mod n$ for Large d.

Let binary reprezentation of the number d be $d[k-1] \ldots d[1]d[0]$.

```
temp=x;
y=1;
for(i=0; i<k; i++)
{if(d[i]==1) y=mod(y*temp,n);
 temp=mod(temp*temp,n);
}
return y;
```



RSA Algorithm– Why Does It Work 1.

Let $x < n$, $y = E(x) = x^e \mod n$.
Does it realy hold that $D(y) = y^d \equiv x \mod n$?
Numbers e, d were chosen such that it holds $e.d \equiv 1 \mod \phi(n)$, i.e. such that $e.d = k.\phi(n) + 1$ for som integer number k.
Therefore

$$\boxed{y^d \equiv (x^e)^d \equiv x^{ed} \equiv x^{k\phi(n)+1} \mod n}$$

1. **If x is coprime with n** then:

$$\begin{aligned} x^{\phi(n)} &\equiv 1 \mod n \\ (x^{\phi(n)})^k &\equiv 1^k \mod n \\ x^{k.\phi(n)} &\equiv 1 \mod n \\ x \cdot x^{k.\phi(n)} &\equiv x \mod n \\ y^d \equiv x^{e.d} \equiv x^{k.\phi(n)+1} &\equiv x \mod n \end{aligned}$$

RSA Algorithm– Why Does It Work 2.

2. **If** x **a** n **are not coprime** then either $p|x$ or $q|x$.

Let $p|x$ then $q \not| x$. (Otherwise it should hold $x = k.pq \geq n$.)

Euler's theorem (for a coprime with q is $a^{\phi(q)} \equiv 1 \mod q$) holds also for $a = x^{\phi(p)}$ since x coprime with q. Then

$$\begin{aligned} (x^{\phi(p)})^{\phi(q)} &\equiv 1 \mod q \\ (x^{\phi(p)})^{k.\phi(q)} &\equiv 1 \mod q \\ x^{k.\phi(p).\phi(q)} &\equiv 1 \mod q \\ x \cdot x^{k.\phi(n)} &\equiv x \mod q \\ x^{k.\phi(n)+1} - x &\equiv 0 \mod q \end{aligned}$$

We have

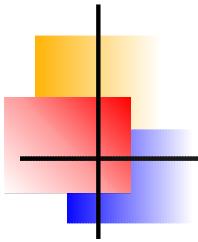
$$x^{k.\phi(n)+1} - x = L.q.$$

Since $p|x$, it has to hold also $p|L$, i.e. $L = M.p$. Therefore it holds

$$x^{k.\phi(n)+1} - x = L.q = M.p.q = M.n \equiv 0 \mod n$$

$$x^{k.\phi(n)+1} - x \equiv 0 \mod n$$

$$x^{k.\phi(n)+1} \equiv x \mod n.$$



Risc of Common n

Let two participants have keys with common modulus n. Some third member send the same message m to both. Message m encipheres into ciphertexts c_1, c_2.

$$\begin{aligned} c_1 &\equiv m^{e_1} \mod n \\ c_2 &\equiv m^{e_2} \mod n \end{aligned}$$

Possible attack:
If e_1, e_2 are coprime we can find r such that $r \cdot e_1 \equiv 1 \mod e_2$.
then it holds:

$$\begin{aligned} r \cdot e_1 - 1 &= s \cdot e_2 \quad \text{for some } s \geq 1 \\ r \cdot e_1 - s \cdot e_2 &= 1 \end{aligned}$$

Let us compute c_3 such that $c_2.c_3 \equiv 1 \mod n$, i.e. $c_3 = c_2^{-1}$.
Then

$$c_1^r.c_3^s \equiv c_1^r.(c_2^{-1})^s \equiv m^{re_1}.m^{-se_2} \equiv m^{re_1 - se_2} \equiv m^1 \equiv m \mod n.$$

Moral: Never encipher the same message two or more times.
Do not use a common modulus n.