(SF2736, Discrete maths, ht15: L4, Thu 5 Nov 2015)

On **a cryptosystem**

$\mathcal{M}$ and $\mathcal{C}$ : Messages (plaintexts) and encrypted messages (ciphertexts),
$E$ and $D$ : Encryption and decryption,

$$\mathcal{M} \underset{D}{\overset{E}{\rightleftarrows}} \mathcal{C} \qquad D(E(m)) = m, \text{ all } m \in \mathcal{M}$$

Traditionally : $E$ and $D$ are only known to the sender and intended recipients.

New (1976) : **Public-key cryptosystems** with $E$ a **one-way function** (i.e., it is very hard to find $D$ knowing $E$), known to "everybody".

**Theorem**: Let $p, q$ be different primes, $n = p \cdot q$, $\;m = (p-1)(q-1)$ $(= \phi(n))$.
Then $\;s \equiv_m 1 \;\Rightarrow\; x^s \equiv_n x,\;$ for all $x \in \mathbb{Z}$

To construct an **RSA system**, for each user do the following:
**Take** $p, q$, large ($\approx 10^{150}$) distinct primes,
**compute** $n = p \cdot q$, $\;m = (p-1)(q-1)$,
**choose** $e$ with $\gcd(e, m) = 1$ and **find** $d$ with $e \cdot d \equiv_m 1$ (use Euclid),
**publish** $(n, e)$ and **keep** $d$ **secret** (throw away $m$ (in secret)).
$E, D : \mathbb{Z}_n \to \mathbb{Z}_n$ with by $E(x) = x^e$ and $D(x) = x^d$ then give $D = E^{-1}$.

$E(x)$ can be **computed** using $f_0, f_1 : \mathbb{Z}_n \to \mathbb{Z}_n$, $f_0(t) = t^2$, $f_1(t) = t^2 \cdot t$:
If $e$ is $(e_k e_{k-1} \ldots e_1 e_0)_2$ in binary,

$$E(x) = f_{e_0}(f_{e_1}(\ldots(f_{e_{k-1}}(f_{e_k}(1)))\ldots)).$$

**Electronic signature** :
1. Send $D(x)$. Anybody with $E$ can read, nobody without $D$ could write.
2. B sends $E_A(D_B(x))$ (or $D_B(E_A(x))$) to A. Only someone with $D_A$ can read (using also $E_B$), only someone with $D_B$ (and $E_A$) could write.

The **Fermat test** (base $b$, $1 < b < N$), to test if $N$ is prime:

$$\boxed{\text{Is } b^{N-1} \equiv_N 1 \;\;?}$$

No : $N$ is composite $\qquad$ Yes : We don't know (for sure)

**Pseudoprime**, base $b$: composite number passing the Fermat test, base $b$.
ex. $341 = 11 \cdot 31$, base 2.

$N$ is a **Carmichael number** iff it is a pseudoprime for **all** $b$ with $\gcd(b, N) = 1$
$\Leftrightarrow$ $N$ is (composite,) square-free and $p \mid N \;\Rightarrow\; (p-1) \mid (N-1)$ (for $p$ prime).
ex. $561 = 3\cdot 11\cdot 17$, $1105 = 5\cdot 13\cdot 17$, $1729 = 7\cdot 13\cdot 19, \ldots, 314\,821 = 13\cdot 61\cdot 397$.

The **Miller-Rabin test** (base $b$, $\;1 < b < N$; $\;N - 1 = u \cdot 2^r$, $\;u$ udda) :

$$\boxed{\text{Is } b^u \equiv_N 1 \text{ or } b^{u\cdot 2^i} \equiv_N -1 \text{ for some } i,\ 0 \le i < r \;\;?}$$

No : $N$ is composite $\qquad$ Yes : We don't know (for sure)

Composite $N$ pass the test for less than $\frac{N}{4}$ of the bases $b$ with $1 < b < N$.

**Strong pseudoprimes**, base $b$: composite, pass the M-Rs test, base $b$.
ex. $2047 = 23 \cdot 89$, base 2.

## On error-correcting codes

A **code** $\mathcal{C}$ is a set of $n$-tuples of 0:s and 1:s, i.e.,

$\mathcal{C} \subseteq V^n, \quad (V = \mathbb{Z}_2 = \{0,1\})$

$n$: the **length** of the code

The **minimal distance** of $\mathcal{C}$:

$\delta = \min\{\partial(a,b) \mid a,b \in \mathcal{C},\ a \neq b\}$

where $\partial(a,b) =$ the number of $i$:s with $a_i \neq b_i$.

$\mathcal{C}$ can **detect** up to $\delta - 1$ errors

and **correct** up to $\left\lfloor \frac{\delta-1}{2} \right\rfloor$ errors. ($\lfloor x \rfloor =$ the integer part of $x =$ the largest integer $\leq x$.)

The **sphere packing bound:**

If the code $\mathcal{C}$, of length $n$, corrects up to $e$ errors,

$$|\mathcal{C}|(\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{e}) \leq 2^n \ (= |\mathbb{Z}_2^n|)$$

$\mathcal{C}$ is a **linear code** if

$$a,b \in \mathcal{C} \Rightarrow a+b \in \mathcal{C}$$

i.e., $\mathcal{C}$ is a **subspace** of the vectorspace $\mathbb{Z}_2^n$ (if $\mathcal{C} \neq \varnothing$)

$|\mathcal{C}| = 2^k$, where $k$ is called (and is) the **dimension** of $\mathcal{C}$.

For a linear code the minimal distance = the **minimal** (non-zero) **weight**,

$$\delta = w_{\min} = \min\{w(c) \mid c \in \mathcal{C},\ c \neq 0\}$$

where the weight of $c$, $w(c)$, is the number of 1:s in $c$.

If $H$ is an $m \times n$-matrix, $\mathcal{C} = \{x \in \mathbb{Z}_2^n \mid Hx = 0\}$ is a linear code of dimension $n - \operatorname{rank} H$. $H$ is called a (parity-)**check matrix**.

**Theorem**: If all columns of $H$ are different and $\neq \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, $\mathcal{C}$ corrects (at least) one error.

To correct errors:

$z$ a code word with error (only) in position $i \ \Rightarrow\ Hz =$ the $i$:th column of $H$.

**Hamming codes** are given by a check matrix $H$ with $r$ rows and $2^r - 1$ columns, all different and $\neq 0$ (so all possible different columns are used)

| | |
|---|---|
| length | $n = 2^r - 1$ |
| minimimal distance | $\delta = 3$ |
| dimension | $k = 2^r - r - 1$ |

Hamming codes give equality in the sphere packing bound. Codes with that property are called **perfect codes**.