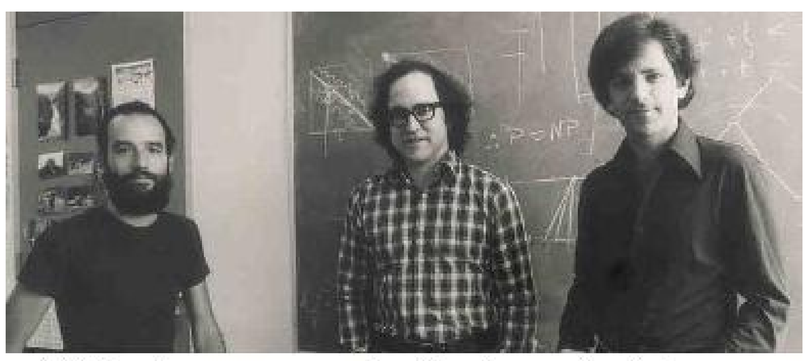
# FACULTE DES SCIENCES

# LE SYSTEME RSA

## Un code à clef publique




Inventé par Rivest, Shamir et Adleman il est aujourd'hui le système à clef publique le plus utilisé (alors que ses inventeurs pensaient démontrer l'impossibilité d'un tel système).

## Code ASCII

Le American Standard Code for Infomation Interchange (ASCII) est un système qui code chaque caractère (lettres, chiffres, ponctuation, espace, ...) par un nombre.

| Char | Dec | Char | Dec | Char | Dec | Char | Dec |
|---|---|---|---|---|---|---|---|
| SPACE | 32 | A | 65 | R | 82 | i | 105 |
| ! | 33 | B | 66 | S | 83 | j | 106 |
| ’ | 39 | C | 67 | T | 84 | k | 107 |
| , | 44 | D | 68 | U | 85 | l | 108 |
| . | 46 | E | 69 | V | 86 | m | 109 |
| 0 | 48 | F | 70 | W | 87 | n | 110 |
| 1 | 49 | G | 71 | X | 88 | o | 111 |
| 2 | 50 | H | 72 | Y | 89 | p | 112 |
| 3 | 51 | I | 73 | Z | 90 | q | 113 |
| 4 | 52 | J | 74 | a | 97 | r | 114 |
| 5 | 53 | K | 75 | b | 98 | s | 115 |
| 6 | 54 | L | 76 | c | 99 | t | 116 |
| 7 | 55 | M | 77 | d | 100 | u | 117 |
| 8 | 56 | N | 78 | e | 101 | v | 118 |
| 9 | 57 | O | 79 | f | 102 | w | 119 |
| : | 58 | P | 80 | g | 103 | x | 120 |
| ? | 63 | Q | 81 | h | 104 | y | 121 |
| é | 130 | à | 133 | è | 138 | z | 122 |

## Les théorèmes utiles

***Théorème de Fermat***

$a^b \equiv a \ mod \ b$, pour $b$ premier.

***Identité de Bézout***

Si $x, y$ sont relativement premiers,
il existe $u, v$ tels que $ux + vy = 1$.

## Le théorème du RSA

Soit $p, q$ premiers et $n = p \cdot q$.
Soit $e$ un nombre premier avec $(p-1) \cdot (q-1)$.
Soit $d$ tel que $e \cdot d \equiv 1 \ mod \ (p-1) \cdot (q-1)$.

$(n, e)$ est la clef publique et $(n, d)$ est la clef privée.
L'expérience montre que la seconde est “difficile” à déduire de la première.

Le codage est $A \mapsto A^e \ mod \ n$ et le decodage est alors $B \mapsto B^d \ mod \ n$.

En effet, pour A entier, le théorème de Fermat implique $A^{ed} \equiv A \ mod \ n$
Donc $(A^e)^d \equiv A^{ed} \equiv A \ mod \ n$ .