

A B C D E F G H I
0 1 2 3 4 5 6 7 8

J K L M N O P Q R S T
9 10 11 12 13 14 15 16 17 18 19
U V W X Y Z
20 21 22 23 24 25

T@N VZ → 4 16 13 21 25
T R T S H → 19 17 19 18 7

$$\begin{array}{r} \text{mod 26} \\ \hline -15 & -1 & -6 & 3 & 18 \\ \hline 11 & 25 & 20 & 3 & 18 \end{array}$$

Om anteckningarna inte räcker till

Adlibris

$$\begin{array}{r}
 4 \ 16 \ 13 \ 21 \ 25 \\
 E Q N V Z \\
 + 1 * 8 * 3 \\
 \hline
 \text{mod 26} \\
 \hline
 5 \quad \quad \quad \quad \quad \quad \\
 \hline
 \text{LAT E R}
 \end{array}$$

L A T E R
 11 0 19 4 17
 \$11 \$0 \$19 \$4 \$17

* \$11 \$0 \$19 \$4 \$17

$$\begin{array}{r}
 4 \ 16 \ 13 \ 21 \ 25 \quad \text{mod 26} \\
 - \$11 \quad \$0 \quad \$19 \quad \$4 \quad \$17 \\
 \hline
 \text{mod 26}
 \end{array}$$

$$4 - x_1 \text{ mod } 26 = 11$$

$$x_1 \text{ mod } 26 = -7$$

$$-7 \text{ mod } 26 = 7$$

Om anteckningarna inte räcker till

Alltid låga priser på studentlitteratur

Adlibris

$$(A - \overset{(-x)}{x_1}) \bmod 26 = 11 \quad -\text{eq 1}$$

$$(B - \overset{(-x)}{x_2}) \bmod 26 = 0 \quad -\text{eq 2}$$

$$(C - \overset{(-x)}{x_3}) \bmod 26 = 19 \quad -\text{eq 3}$$

$$(D - \overset{(-x)}{x_4}) \bmod 26 = 4 \quad -\text{eq 4}$$

$$(E - \overset{(-x)}{x_5}) \bmod 26 = 17 \quad -\text{eq 5}$$

T Q U R I is the key. we roll back
from 2 to A for negative index.

T Q U R I	16 13 21 25 7 4 11 11 14 14 + 19 16 20 17 8 26 20 31 18 22 0 20 5 18 22 A U F S W
-----------------------	--

mod 26

Verification

$\oplus N \sqrt{2}$	4	16	13	21	25	$(\oplus N \sqrt{2})$
T A U R I	- 19	16	20	17	8	(T A U R I)
	<u> </u>					
	- 15	0	7	9	17	
	↓	↓	↓	↓	↓	
mod 21	11	0	19	1	17	
	↓	↓	↓	↓	↓	
	L	A	T	E	R	

(83)

$$p=7, q=11$$

$$N = p \times q = 7 \times 11 = 77$$

$$w = (p-1) \times (q-1) = (7-1) \times (11-1) = 6 \times 10 = 60$$

$e = ?$

''' Public Exponent e : $e < w \wedge e$ is relatively prime. to w .

$e = 17$ chosen

$d = ?$

$$d = e^{-1} \bmod 60$$

$$d = 17^{-1} \bmod 60$$

$$d = \frac{1}{17} \bmod 60$$

$$d = e^{-1} \bmod w$$

$$= 17^{-1} \bmod 60$$

$$= 53$$

$$17^{-1} \bmod 60 = 53$$

Public Key = { N, e } = {77, 17}

Private Key = { N, d } = {77, 53}

Encryption $\Rightarrow C = M^e \bmod N$

Decryption $\Rightarrow D = C^d \bmod N$

Example message $\Rightarrow M = 65$

$$\text{Encrypt} \Rightarrow C = 65^{17} \bmod 77 = 32$$

$$\text{Decrypt} \Rightarrow D = 32^{53} \bmod 77 = 65$$

Om anteckningarna inte räcker till

Alltid låga priser på studentlitteratur

Adlibris