Problem 5

You found a ciphertext **Y=46**. It is encrypted by the **RSA cryptosystem** with parameter **N=91** and (public) encryption key **E=29**. What is the plaintext X?

Ronald Linn Rivest
(1947-)

Adi Shamir
(1952-)

Leonard Adleman
(1945-)

https://en.wikipedia.org/wiki/Ron_Rivest
https://en.wikipedia.org/wiki/Adi_Shamir
https://en.wikipedia.org/wiki/Leonard_Adleman

Problem 5

RSA cryptosystem

Parameter	**N=91**
(Public) Encryption Key	**E=29**
Ciphertext	**Y=46**

- Given a plaintext X, the ciphertext Y is calculated by $\mathbf{Y \equiv X^E \pmod{N}}$.
- We need to solve $\mathbf{46 \equiv X^{29} \pmod{91}}$.

Problem 5

- **Factorize** $N=P\times Q$. $91=7\times 13$
- Calculate $(P-1)\times(Q-1)$. $6\times 12=72$
- Calculate **mult inverse** D of $E=29 \pmod{72}$.

$$5\times 29 \equiv 1 \pmod{72}$$

- **Decryption key** $D=5$. Calculate $Y^D \pmod{N}$.

$$46^5 \equiv 37 \pmod{91}$$

Answer The plaintext is $X=37$.

(Confirm $37^{29} \equiv 46 \pmod{91}$.)

Problem 5

A possible attack to RSA

(1) (**Difficult**) **Factorize N=P×Q**.

(2) (Easy by Euclidean Algorithm) Calculate the mult inverse D of E (mod (P−1)(Q−1)).

(3) (Easy) Calculate Y^D (mod N).

Ronald Linn Rivest (1947-)

Adi Shamir (1952-)

Leonard Adleman (1945-)