Popa Alex Ovidiu
936

23.10.2020

PKC Assignment A

(02)

$n_1 = 2957$, primality of n_1 using Miller-Rabin test

$n_1 - 1 = 2957 - 1 = 2956 = 2^2 \cdot 739$

$\Rightarrow s = 2 \quad t = 739$

<u>$k=1$</u>, pick $a = 2$

Compute $2^{739}, 2^{2\cdot 739}, 2^{2^2 \cdot 739} \pmod{2957}$

$2^{739} = ? \pmod{2957}$

$739 = 512 + 128 + 64 + 32 + 2 + 1$
$= 2^9 + 2^7 + 2^6 + 2^5 + 2^1 + 2^0$

- show all steps for repeated squaring modular exp.

$2^{2^0} = 2 \pmod{2957}$

$2^{2^1} = 4 \pmod{2957}$

$2^{2^2} = 4 \cdot 4 = 16 \pmod{2957}$

$2^{2^3} = 2^{(2^2)} \cdot 2^{(2^2)} = 16^2 = 256 \pmod{2957}$

$2^{2^4} = 256^2 = 482 \pmod{2957}$

$2^{2^5} = 2^{(2^4)} \cdot 2^{(2^4)} = 482 \cdot 482 = 1678 \pmod{2957}$

$2^{2^6} = 2^{(2^5)} \cdot 2^{(2^5)} = 1678 \cdot 1678 = 620 \pmod{2957}$

Scanned with CamScanner

$2^{2^7} = 2^{(2^6)} \cdot 2^{(2^6)} = 620 \cdot 620 = 2947 \pmod{2957}$

$2^{2^8} = 2^{(2^7)} \cdot 2^{(2^7)} = 2947 \cdot 2947 = 100 \pmod{2957}$

$2^{2^9} = 2^{(2^8)} \cdot 2^{(2^8)} = 100 \cdot 100 = 1129 \pmod{2957}$

$\Rightarrow 2^{739} = 2^{2^0 + 2^1 + 2^5 + 2^6 + 2^7 + 2^9}$

$2^{739} = 2 \cdot 4 \cdot 1678 \cdot 620 \cdot 2947 \cdot 1129$

$2^{739} = 1222 \pmod{2957}$

$2^{2 \cdot 739} = (2^{739})^2 = 1222^2 = -1 \pmod{2957}$

$2^{2^2 \cdot 739} = (2^{2 \cdot 739})^2 = (-1)^2 = 1 \pmod{2957}$

The sequence is $1222, -1, 1$, hence $n_1 = 2957$ is possible to be prime, and we will try another base.

$k=2$, pick $a=3$

Compute $3^{739}, 3^{2 \cdot 739}, 3^{2^2 \cdot 739} \pmod{2957}$

- show computation for $3^{739} \bmod 2957$ using repeated squaring modular exponentiation

$3^{2^0} = 3 \pmod{2957}$

$3^{2^1} = 3^{(2^0)} \cdot 3^{(2^0)} = 9 \pmod{2957}$

$3^{2^2} = 3^{(2^1)} \cdot 3^{(2^1)} = 81 \pmod{2957}$

$3^{2^3} = 3^{(2^2)} \cdot 3^{(2^2)} = 81 \cdot 81 = 647 \pmod{2957}$

$3^{2^4} = 3^{(2^3)} \cdot 3^{(2^3)} = 647 \cdot 647 = 1672 \pmod{2957}$

$3^{2^5} = 3^{(2^4)} \cdot 3^{(2^4)} = 1672 \cdot 1672 = 1219 \pmod{2957}$

$3^{2^6} = 3^{(2^5)} \cdot 3^{(2^5)} = 1219 \cdot 1219 = 1547 \pmod{2957}$

$3^{2^7} = 3^{(2^6)} \cdot 3^{(2^6)} = 1547 \cdot 1547 = 996 \pmod{2957}$

$3^{2^8} = 3^{(2^7)} \cdot 3^{(2^7)} = 996 \cdot 996 = 1421 \pmod{2957}$

$3^{2^9} = 3^{(2^8)} \cdot 3^{(2^8)} = 1421 \cdot 1421 = 2567 \pmod{2957}$

$3^{739} = 3^{2^0 + 2^1 + 2^5 + 2^6 + 2^7 + 2^9}$

$= 3 \cdot 9 \cdot 1219 \cdot 1547 \cdot 996 \cdot 2567$

$3^{739} = 1222 \pmod{2957}$

$3^{2 \cdot 739} = (3^{739})^2 = 1222^2 = -1 \pmod{2957}$

$3^{2^2 \cdot 739} = (3^{2 \cdot 739})^2 = (-1)^2 = 1 \pmod{2957}$

Again, $n = 2957$ is possible to be prime, as the sequence is $1222, -1, 1$, so we will try one last base.

(3)

$k=3$, pick $a=5$

Compute $5^{739}, 5^{2\cdot 739}, 5^{2^2\cdot 739} \pmod{2957}$

$5^{2^0} = 5 \pmod{2957}$

$5^{2^1} = 5\cdot 5 \pmod{2957} = 25$

$5^{2^2} = 25\cdot 25 = 625 \pmod{2957}$

$5^{2^3} = 5^{(2^2)}\cdot 5^{(2^2)} = 625\cdot 625 = 301 \pmod{2957}$

$5^{2^4} = 5^{(2^3)}\cdot 5^{(2^3)} = 301\cdot 301 = 1891 \pmod{2957}$

$5^{2^5} = 5^{(2^4)}\cdot 5^{(2^4)} = 1891\cdot 1891 = 868 \pmod{2957}$

$5^{2^6} = 5^{(2^5)}\cdot 5^{(2^5)} = 868\cdot 868 = 2346 \pmod{2957}$

$5^{2^7} = 5^{(2^6)}\cdot 5^{(2^6)} = 2346\cdot 2346 = 739 \pmod{2957}$

$5^{2^8} = 5^{(2^7)}\cdot 5^{(2^7)} = 739\cdot 739 = 2033 \pmod{2957}$

$5^{2^9} = 5^{(2^8)}\cdot 5^{(2^8)} = 2033\cdot 2033 = 2160 \pmod{2957}$

$5^{739} = 5^{2^0+2^1+2^5+2^6+2^7+2^9}$

$= 5\cdot 25\cdot 868\cdot 2346\cdot 739\cdot 2160 \pmod{2957}$

$5^{739} = 1222$

$5^{2\cdot 739} = (5^{739})^2 = 1222^2 = -1 \pmod{2957}$

$5^{2^2\cdot 739} = (5^{2\cdot 739})^2 = (-1)^2 = 1 \pmod{2957}$

The sequence is $1222, -1, 1$, so $n = 2957$ is probable to be prime, since we've reached the end of the third base, i.e. $k=3$.

$\Rightarrow$ The probability of having an error is

$$P < \frac{1}{64}$$

$n_2 = 161$

$n_2 - 1 = 161 - 1 = 160 = 2^5 \cdot 5$

$\Rightarrow s = t = 5$

Miller - Rabin test $\to k = 1, a = 2$

Compute $2^5, 2^{2^1 \cdot 5}, 2^{2^2 \cdot 5}, 2^{2^3 \cdot 5}, 2^{2^4 \cdot 5}, 2^{2^5 \cdot 5}$ (mod 161)

$2^5 = 2^{4+1} = 2^4 \cdot 2^1 = 16 \cdot 2 = 32 \pmod{161}$

(short version of showing the computations for computing 2^5 mod 161 using the repeated squaring modular exp.)

$2^{2 \cdot 5} = (2^5)^2 = 32^2 = 58 \pmod{161}$

$2^{2^2 \cdot 5} = (2^{2 \cdot 5})^2 = 58^2 = 144 \pmod{161}$

$2^{2^3 \cdot 5} = (2^{2^2 \cdot 5})^2 = 144^2 = 128 \pmod{161}$

$2^{2^4 \cdot 5} = (2^{2^3 \cdot 5})^2 = 128^2 = 123 \pmod{161}$

$2^{2^5 \cdot 5} = (2^{2^4 \cdot 5})^2 = 123^2 = 156 \pmod{161}$

The sequence is: 32, 58, 144, 128, 123, 156, and we've reached the end of the algorithm which means that $n_2 = 161$ is composite.