Gloire Rubambiza
04/11/2018
MTH 312 - 01

Assessment 4 Preparation

1. Find an integer n, $0 \le n < 1820$, so that:

$$n \bmod 65 = 51$$
$$n \bmod 18 = 3$$

Plan: Find numbers n_1 and n_2 so that

$n_1 \bmod 65 = 1$ $\quad$ $n_2 \bmod 65 = 0$

$n_1 \bmod 18 = 0$ $\quad$ $n_2 \bmod 18 = 1$

then

$$(51n_1 + 3n_2) \bmod 65 = 51$$
$$(51n_1 + 3n_2) \bmod 18 = 3$$

Then calculate $(51n_1 + 3n_2) \bmod (65 \cdot 18)$

$$\begin{bmatrix} 65 \\ 1 \\ 0 \end{bmatrix} - 3\begin{bmatrix} 18 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 11 \\ 1 \\ -3 \end{bmatrix}$$

$$\begin{bmatrix} 18 \\ 0 \\ 1 \end{bmatrix} - \begin{bmatrix} 11 \\ 1 \\ -3 \end{bmatrix} = \begin{bmatrix} 7 \\ -1 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix} 11 \\ 1 \\ -3 \end{bmatrix} - \begin{bmatrix} 7 \\ -1 \\ 4 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \\ -7 \end{bmatrix}$$

$$\begin{bmatrix} 7 \\ -1 \\ 4 \end{bmatrix} - \begin{bmatrix} 4 \\ 2 \\ -7 \end{bmatrix} = \begin{bmatrix} 3 \\ -3 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} 4 \\ 2 \\ -7 \end{bmatrix} - \begin{bmatrix} 3 \\ -3 \\ 11 \end{bmatrix} = \begin{bmatrix} 1 \\ 5 \\ -18 \end{bmatrix}$$

So $5 \cdot 65 - 18 \cdot 18 = 1$

$-18 \cdot 18 = 1 - 5 \cdot 65$

$-18 \cdot 18 \bmod 65 = 1$

$-18\ 18 \bmod 18 = 0$

$\Rightarrow n_1 = (-18)(18)$

$5 \cdot 65 \bmod 65 = 0$

$5 \cdot 65 \bmod 18 = (1 + 18 \cdot 18) \bmod 18$

$= 1$

$n_2 = 5 \cdot 65$

$51(-18 \cdot 18) + 3(65 \cdot 5) = -15549$

$-15549 \bmod 65 = -14 \equiv 51 \bmod 65$ ✓

$-15549 \bmod 18 = -15 \equiv 3 \bmod 18$ ✓

↳ Not in range $0 \le n < 1820$, so $n = -15549 \bmod 1820 = -989 \equiv 831 \bmod 1820$

$n = 831$

Gloire Rubambiza
04/11/2018
MTH 312-01

Assessment 4 Preparation

2. Use Fermat's factorization method to find the primes p and q so that $pq = 79927$

$a = \text{ceiling}(\sqrt{79927}) = 283$

Try 1: $b^2 = a^2 - 79927 = 283^2 - 79927 = 162$ ✗

Try 2: $b^2 = (284)^2 - 79927 = 729$ ✓ perfect square

$\Rightarrow b = 27$

$p = a - b = 284 - 27 = 257$

$q = a + b = 284 + 27 = 311$

Gloire Rubambiza
04/11/2018
MTH 312-01

Assessment 4 Preparation

RSA

8.a) $m = 14921$
$M = 79927$
$e = 12589$
$n = m^e \bmod M$
$n = 14921^{12589} \bmod 79927$

$14921^{12589} = 14921^{8192+4096+256+32+16+8+4+1}$

$14921^{1} \bmod 79927 = 14921$ *
$14921^{2} \bmod 79927 = 39546$ *
$14921^{4} \bmod 79927 = 39546^2 \bmod 79927 = 34434$ *
$14921^{8} \bmod 79927 = 34434^2 \bmod 79927 = 63238$ *
$14921^{16} \bmod 79927 = 63238^2 \bmod 79927 = 57053$ *
$14921^{32} \bmod 79927 = 57053^2 \bmod 79927 = 17734$ *
$14921^{64} \bmod 79927 = 17734^2 \bmod 79927 = 61938$
$14921^{128} \bmod 79927 = 61938^2 \bmod 79927 = 59625$
$14921^{256} \bmod 79927 = 59625^2 \bmod 79927 = 67592$ *
$14921^{512} \bmod 79927 = 67592^2 \bmod 79927 = 51144$
$14921^{1024} \bmod 79927 = 51144^2 \bmod 79927 = 17734$
$14921^{2048} \bmod 79927 = 17734^2 \bmod 79927 = 61938$
$14921^{4096} \bmod 79927 = 61938^2 \bmod 79927 = 59625$ *
$14921^{8192} \bmod 79927 = 59625^2 \bmod 79927 = 67592$ *

$\Rightarrow 14921^{12589} = (67592)^2 (59625)(17734)(57053)(63238)(34434)(39546)(14921) \bmod 79927$

$\Rightarrow$ Using the multiple squaring program from class $\boxed{n = 24,226}$

Gloire Rubambiza
04/11/2018
MTH 312-01

Assessment 4 Preparation

RSA

8.b) Find the Decryption (private) key corresponding to the public key

$n = 1319 \cdot 1129$, $e = 12589$, $d = ?$

$\varphi = (p-1)\cdot(q-1) = (1318)(1128) = 1486704$

Assume $\gcf(e, \varphi) = 1$ and $d \cdot e + k \cdot \varphi = 1$

$\Rightarrow 1 = d \cdot 12589 + k \cdot 1486704$

$d \cdot 12589 = (-k) \cdot 1486704 + 1$

so

$d \cdot 12589 \bmod 1486704 = 1$

$1486704 = 118 \cdot 12589 + 1202$

$$\begin{bmatrix}1486704\\1\\0\end{bmatrix} - 118\begin{bmatrix}12589\\0\\1\end{bmatrix} = \begin{bmatrix}1202\\1\\-118\end{bmatrix}$$

$$\begin{bmatrix}12589\\0\\1\end{bmatrix} - 10\begin{bmatrix}1202\\1\\-118\end{bmatrix} = \begin{bmatrix}569\\-10\\1181\end{bmatrix}$$

$$\begin{bmatrix}1202\\1\\-118\end{bmatrix} - 2\begin{bmatrix}569\\-10\\1181\end{bmatrix} = \begin{bmatrix}64\\21\\-2480\end{bmatrix}$$

$$\begin{bmatrix}569\\-10\\1181\end{bmatrix} - 8\begin{bmatrix}64\\21\\-2480\end{bmatrix} = \begin{bmatrix}57\\-178\\21021\end{bmatrix}$$

$$\begin{bmatrix}64\\21\\-2480\end{bmatrix} - 1\begin{bmatrix}57\\-178\\21021\end{bmatrix} = \begin{bmatrix}7\\-199\\-23501\end{bmatrix}$$

$$\begin{bmatrix}57\\-178\\21021\end{bmatrix} - 8\begin{bmatrix}7\\-199\\-23501\end{bmatrix} = \begin{bmatrix}1\\-1770\\209029\end{bmatrix}$$

$\Rightarrow 1 = -1770 \cdot 1486704 + 209029 \cdot 12589$

Hence d = multiplicative inverse of $e = 209029$

Gloire Rubambiza
04/12/2018
MTH 312-01

Assessment 4 Preparation

8. c) $M = 79927$, $e = 48563$, $d = 20347$.

$n = 75375$, $c = ?$

$c = n^d \bmod M$

$c = 75375^{20347} \bmod 79927$

$\boxed{c = 13775}$