DAY: 18 DATE:

RSA:

Prime numbers = 17, 19

encrypt text = 13

$17 \times 19 = 323 \rightarrow n$

$16 * 18 = 288 \rightarrow \phi(n)$

$1 < e < \phi(n)$

$(\phi(n), e) = \gcd = 1$

$e = 7$

$(288, e) = \gcd(288, e) = 1$

$C = m^e \bmod n$

text

$= 13^7 \bmod 323$

$= 276$

$e^{-1} \rightarrow d \rightarrow 247$

$m = c^d \bmod n$

$d = e^{-1} \bmod \phi(n)$

DAY: DATE:

$276^{247} \% 323 = 13$

→ implement RSA in any lang.

$n = 2537$

$d = 937$

$C = 855$

$M = C^d \bmod n$

$M = 855^{937} \% 2537$

$m = 2077$

$n = 33$

$d = 7$

$C = 16$

813407

DAY: DATE:

$m = 16^7 \mod 33$

$m = 25$

17, 23

$m = 88$

$n = 17 \times 23 = 391$

$\phi(n) = 352$

$1 < e < 352$

$\downarrow$

3

$c = m^e \mod n$

$= 88^3 \mod 391$

$c = 350$

88

$d = e^{-1} \mod \phi(n) = 235$

$m = c^d \mod n = 350^{235} \mod 391$