$Z = 5$

	1	2	3	4
1^Y	1	2	3	4
2^Y	2	4	3	1
3^Y	3	4	2	1
4^Y	4	1	4	1

$3^5 = 3^{4+1} = 3^4 \cdot 3^1$ (1 * 3)

$= 3^2 \cdot 3^2 \cdot 3^1$

3^1 % 5 = 3

3^2 = 4

3^4 = 1

$3^7 = 3^{4+2+1} = 3^4 \cdot 3^2 \cdot 3^1$

$\Rightarrow 1 * 4 * 3 \,\%\, 5$

$= 2$

$3^{12} = 3^{8+4} = 3^4 \cdot 3^4 \cdot 3^4$

$\Rightarrow 1 \cdot 1 \cdot 1 \Rightarrow 1$

$Z_n^* = \{ x \in Z_n , \gcd(x, n) = 1 \}$

$Z_{10}^* = \{1, 3, 7, 9\}$

$Z_{13}^* = Z_n - \{n\}$; n is prime

$\phi(n)$ is the totient of Z_n^*'s size

$\phi(10) = 4$

$\phi(n) = n(1 - \frac{1}{P_1}) \cdots (1 - \frac{1}{P_m})$

$P_1 \cdots P_m$ = prime factors

$\phi(38) = 38(1 - \frac{1}{2})(1 - \frac{1}{19})$

$= 38 \cdot \frac{18}{19} \cdot \frac{1}{2}$

$= 18$

$M = 4$, Public key $(e, n) = (3, 77)$ RSA encryption

$C_1 = M^e \bmod n$

$= 4^3 \bmod 77$

$= 64 \,\%\, 77$

$= 64$

$p = 17 \quad q = 11 \quad e = 7$

① $n = pq = 187$

② $\phi = 160 = (p-1)(q-1)$

③ select $e = 7$

④ compute

$$d = e^{-1} \bmod \phi(n)$$
$$= 7^{-1} \bmod 160$$
$$= 23$$
$$(7^{-1} \cdot 23) \bmod 160 = 1$$

$P\ (7, 187)$ RSA public key

$S\ (23, 187)$ RSA private key

$M = 5$

$5^7 \bmod 187$

$P = (7, 187), \quad m = 88$ (e, n)

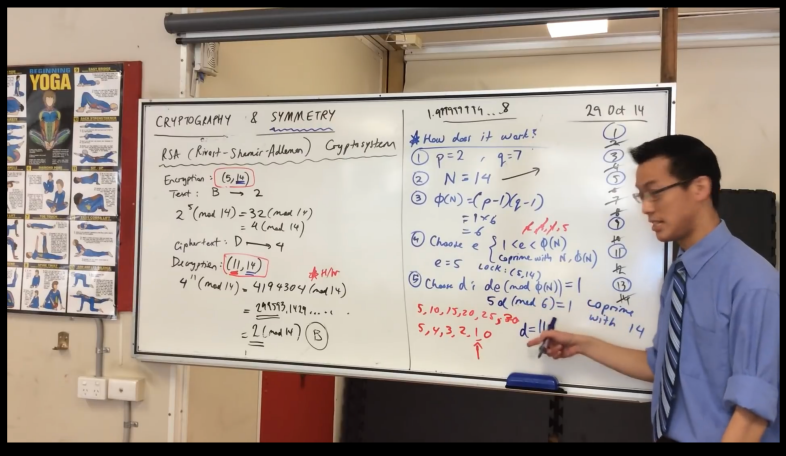
7744

$88 \Rightarrow 88$

$88^2 \Rightarrow 77$

$88^4 \Rightarrow 132$

$$c_1 = m_1^e \bmod n$$
$$= 88^7 \bmod 187$$
$$= 88^{4+2+1} \bmod 187$$
$$= ((132 \cdot 77 \bmod 187) \bmod 187)$$
$$=$$



$(23-37)\%5$

$-14 \%_{n} 5 = -4_{b}$ (a)

$a = b \pmod n$

$a - b = kn$

$-14 - (-4) = (-2) * 5$

$-14 - 1 =$

$77^7 \bmod 160$

$77 \longrightarrow 77$

$77^2 \longrightarrow 9$

$77^3 \longrightarrow 53$

$77^4 \longrightarrow 81$

$77^7 = 77^{4+2+1}$

$= 77^4 \cdot 77^2 \cdot 77 \bmod 160$

$= 81 * 9 * 77 \bmod 160$

$= 133$

write ↓

problem title	writer	helper

writer references Member(role)

CHECK (writer == PC OR ~~writer == Null~~)

CHECK writer IN (
SELECT role from Member
)