(d) $(e_A, n_A) = (53, 10961)$

$(e_B, n_B) = (971, 10807)$

$C = 9988$

1. Déterminer : $n_A < n_B$ ou $n_A > n_B$?

2. Déduire :

cas 1 : $C_1 = C^{d_B} \bmod n_B$ puis $M = C_1^{e_A} \bmod n_A$

cas 2 : $C_1 = C^{e_A} \bmod n_A$ puis $M = C_1^{d_B} \bmod n_B$

→ Calculer $d_B \iff [e_B]^{-1}_{\varphi(n_B)}$

1. ici, $n_A > n_B$

2. $C_1 = C^{e_A} \bmod n_A$

$M = C_1^{d_B} \bmod n_B$

$d_B \iff [e_B]^{-1}_{\varphi(n_B)}$

$n_B = 10807 = 101 \cdot 107$ ← est un produit de facteurs premiers

$\varphi(n_B) = \varphi(101) \cdot \varphi(107)$ ← Ce sont systématiquement des φ de facteurs premiers

$= 100 \cdot 106$

$= 10600$

$d_B = [971]^{-1}_{10600}$

3. Résoudre d_B par remontée Algo Euclide

e_B — $\varphi(n_B) \to 10600 = 10 \cdot 971 + 890$ (r_1)

$971 = 890 + 81$ (r_2)

$890 = 10 \cdot 81 + 80$ (r_3)

$81 = 80 + 1$ (r_4)

$1 = -12\varphi(n_B) + n e_B + 12 e_B = -12\varphi(n_B) + 131 e_B$

$1 = -12 r_1 + n e_B = n e_B - 12(\varphi(n_B) - 10 e_B)$

$1 = -r_1 + n r_2 = -r_1 + n(e_B - r_1)$

$1 = r_2 - r_3 = r_2 - (r_1 - 10 r_2)$

$d_B = 131$

4. $C_1 = C^{e_A} \bmod n_A$ → Décomposer e_A en puissance de 2

$e_A = 53$ soit $e_A = 2^5 + 2^4 + 2^2 + 1$ ← $1 = C$

C	C^2	C^{2^2}	C^{2^3}	C^{2^4}	C^{2^5}
9988	4083	10169	2487	3165	9832

$\to \bmod 10961$

c'est $9988^2 \% 10961$

5. Déduire en multipliant

$C_1 = C \cdot C^{2^2} \cdot C^{2^4} \cdot C^{2^5}$

$= 9988 \cdot 10169 \cdot 3165 \cdot 9832$

c'est $9988 \cdot 10169 \% 10961$ $= 3346 \cdot 1$

$= 3346$

6. Découvrir le message en résolvant M

6.1 Décomposer d_B en puissance de 2

$d_B = 131 = 2^7 + 2^1 + 1 \longleftrightarrow C = 1$

C_1	C_1^2	$C_1^{2^2}$	$C_1^{2^3}$	$C_1^{2^4}$	$C_1^{2^5}$	$C_1^{2^6}$	$C_1^{2^7}$
3346	10471	4825	1191	2764	9959	3540	6287

$M = 3346 \cdot 10471 \cdot 6287 \bmod 10807$

$M = 10479 \cdot 6287 \bmod 10807$

$M = \underline{2001}$ ✓

message déchiffré