1.1 DES for 64 bit encryption only has 2^{56} space complexity

$x \in \mathcal{M}$, $k_i \in \mathcal{K}$, $c_i \in \mathcal{C}$

$$\begin{cases} C_1 = Enc(k_1, x) & \Rightarrow 2^{56} \\ C_2 = Enc(k_2, C_1) & \Rightarrow 2^{112} \\ C_3 = Enc(k_3, C_2) & \Rightarrow 2^{168} \end{cases}$$

but $C' = Enc(k', x)$ only 2^{56}

if we want to find a pair (k', x) to break C_3, the probability is

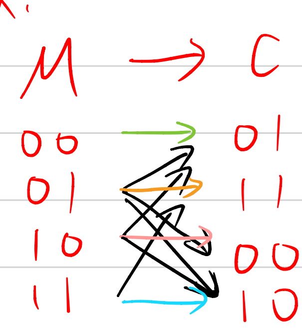
$$\frac{2^{56}}{2^{168}} = \frac{1}{2^{112}} \approx 0 \quad \text{negligible}$$ ※

以上是考慮存在所有k'對應到所有(k_1, k_2, k_3)的機率，
但實際上不可能

Assume DES has 64-bit (ignore parity bit)

$|\mathcal{K}| = 2^{64}$, 但 $|\mathcal{M}| \rightarrow |\mathcal{C}|$ 有 $2^{64}!$ 種可能

ex.



2 bits

$4 \times 3 \times 2 \times 1 = 4! = 2^2!$

For 3DES

$$|\mathcal{M}| \rightarrow |\mathcal{C}_1| \rightarrow |\mathcal{C}_2| \rightarrow |\mathcal{C}_3|$$

$$2^{64} \qquad 2^{64}! \times 2^{64}! \times 2^{64}!$$

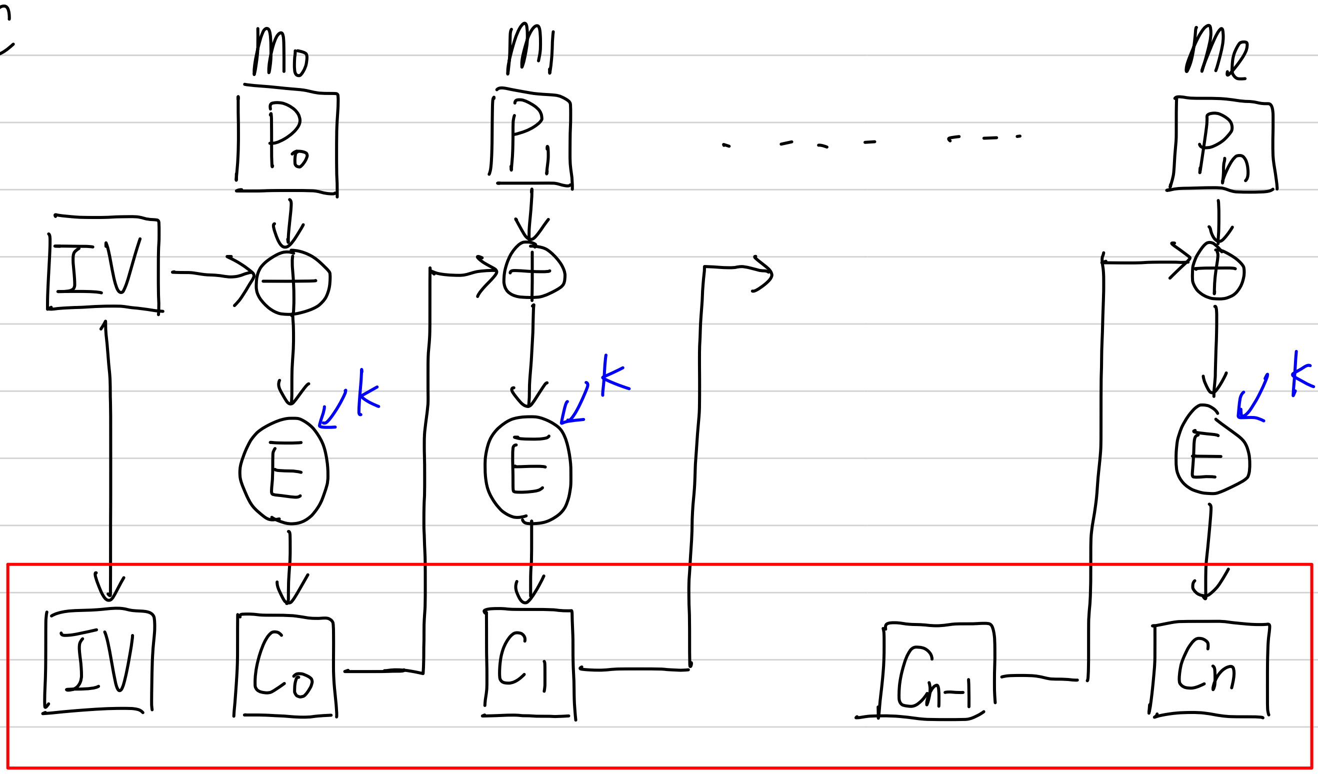
$(2^{64}!)^3$ 種

所以 k' 是不可能存在的

1.2 略；大家都會

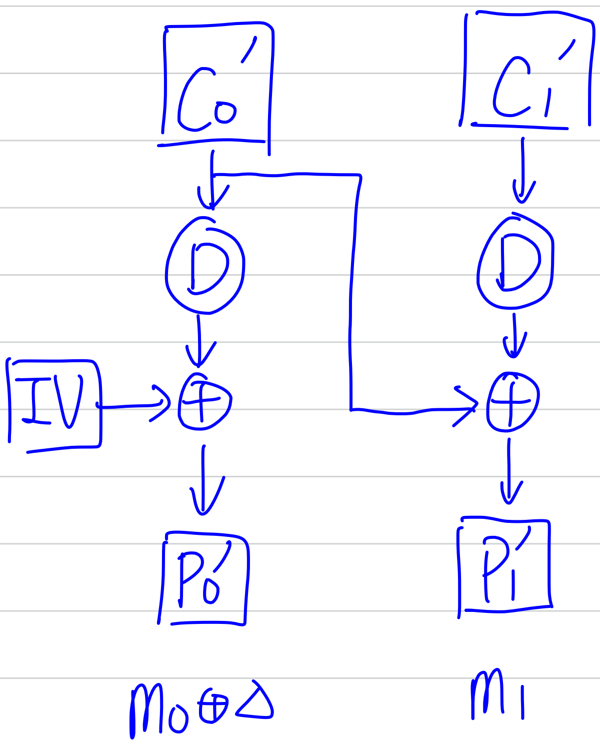
1.3

CBC



$\Downarrow$

C



modify IV with $IV \oplus \Delta$

(that's why WEP is not secure in wifi protocol)

1.4

(a)

$$997 = 400 \times 2 + 197$$
$$400 = 197 \times 2 + 6$$
$$197 = 6 \times 32 + 5$$
$$6 = 5 \times 1 + 1$$

$\Rightarrow$

$$\begin{aligned} 1 &= 6 - 5 \times 1 \\ &= 6 \times 33 - 197 \\ &= 400 \times 33 - 197 \times 67 \\ &= 400 \times 167 - 997 \times 67 \end{aligned}$$

$$400^{-1} \bmod 997 \equiv 167$$ ※

(b)

$$16651 = 472 \times 35 + 131$$
$$472 = 131 \times 3 + 79$$
$$131 = 79 \times 1 + 52$$
$$79 = 52 \times 1 + 27$$
$$52 = 27 \times 1 + 25$$
$$27 = 25 \times 1 + 2$$
$$25 = 2 \times 12 + 1$$

$\Rightarrow$

$$\begin{aligned} 1 &= 25 - 2 \times 12 \\ &= 25 \times 13 - 27 \times 12 \\ &= 52 \times 13 - 27 \times 25 \\ &= 52 \times 38 - 79 \times 25 \\ &= 131 \times 38 - 79 \times 63 \\ &= 131 \times 227 - 472 \times 63 \\ &= 16651 \times 227 - 472 \times 8008 \end{aligned}$$

$$\begin{aligned} 472^{-1} \bmod 16651 &\equiv -8008 \\ &\equiv 8643 \end{aligned}$$ ※

1.5 ① $m = kp \Rightarrow m \cdot m^{\phi(N)} \equiv m \cdot m^{\phi(p)\phi(q)} \equiv m \mod q$

$\Rightarrow m \cdot m^{\phi(N)} \equiv 0 \mod p$

② 同理 $m = kq \Rightarrow m \cdot m^{\phi(N)} \equiv m \mod p$

$m \cdot m^{\phi(N)} \equiv 0 \mod q$

③ 中國剩餘定理 $\Rightarrow m \cdot m^{\phi(N)} \equiv m \mod N$

1.6

RSA requires:

① p, q coprime and $p \neq q$

② p, q pass Fermat's little theorem (FLT)

$\Rightarrow$ p, q are called Carmichael number

You can try $p = \overset{3\times11\times17}{561}$ $q = \overset{7\times11\times13\times41}{41041}$, this case is all wrong.

$e = 257$, $d = pow(e, -1, \phi(N))$ $N = p \cdot q$

Another case $p = \overset{7\times11\times13\times41}{41041}$ $q = \overset{3\times5\times47\times89}{62745}$

$e = 127$ $d = pow(e, -1, \phi(N))$ $N = p \cdot q$

this case is all correct

1.7

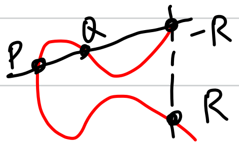
$y^2 \equiv (x^3+ax+b) \bmod p$

prove $\begin{cases} x_R = (\lambda^2 - x_P - x_Q) \bmod p \\ y_R = (\lambda(x_P - x_R) - y_P) \bmod p \end{cases}$

where $\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & \text{if } P \neq Q \\ \dfrac{3x_P^2 + a}{2y_P} & \text{if } P = Q \end{cases}$

because $R = P + Q$

$\Rightarrow$ $P, Q, -R$ are at the same line



(add minus sign)

let $y = mx + n$ pass through P, Q if $P \neq Q$

$\Rightarrow \begin{cases} y_P = mx_P + n \\ y_Q = mx_Q + n \end{cases}$ $\quad m = \dfrac{y_P - y_Q}{x_Q - x_P}$ $\quad -y_R = mx_R + n$, too

$n = y_P - \dfrac{y_P - y_Q}{x_Q - x_P} x_P$

also $\begin{cases} y_R^2 = x_R^3 + ax_R + b \\ -y_R = mx_R + n \end{cases}$ $\Rightarrow (mx_R + n)^2 = x_R^3 + ax_R + b$

$\Rightarrow m^2 x_R^2 + n^2 + 2mn x_R = x_R^3 + ax_R + b$

$\Rightarrow x_R^3 - m^2 x_R^2 + (a - 2mn) x_R + (b - n^2) = 0$

比較

We know x_P, x_Q, x_R are the roots of the equation

$\Rightarrow (x - x_P)(x - x_Q)(x - x_R) = 0$ (三次方係數為 1)

$\Rightarrow x^3 - \underbrace{(x_P + x_Q + x_R)}_{= m^2} x^2 + (x_P x_Q + x_Q x_R + x_P x_R) x - x_P x_Q x_R = 0$

①

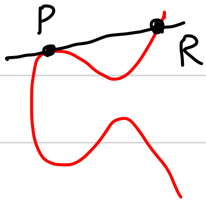
$x_P + x_Q + x_R = m^2 \Rightarrow x_R = m^2 - x_P - x_Q$, m here is λ

②

$\begin{matrix} y_P = mx_P + n \\ -y_R = mx_R + n \end{matrix} \Rightarrow y_P + y_R = m(x_P - x_R) \Rightarrow y_R = m(x_P - x_R) - y_P$

m here is λ

if $P = Q \Rightarrow$



we have to know the slope of P

$\Rightarrow y^2 = x^3 + ax + b$ derived by x

$\Rightarrow 2y\dfrac{dy}{dx} = 3x^2 + a$ substitute (x_P , y_P)

$$\Rightarrow \left.\frac{dy}{dx}\right|_P = \frac{3x_P + a}{2y_P}$$