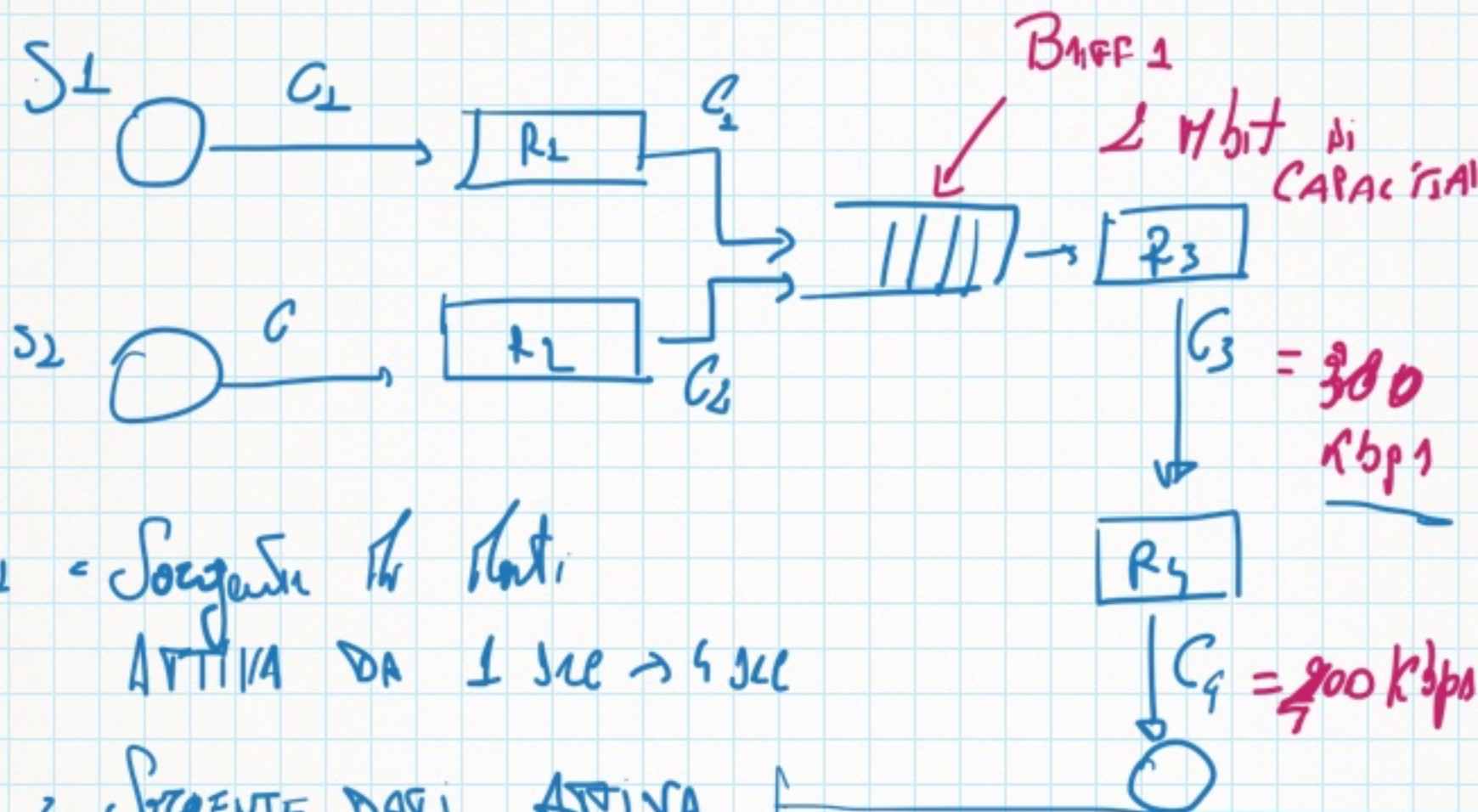




S_1 = Sorgente in Attiva
ATTIVA DA 1 sec $\rightarrow$ 4 sec

S_2 = Sorgente dati ATTIVA
DA 1 $\rightarrow$ 10 sec

$S_1 = 300 \text{ kbps}$

$S_2 = 150 \text{ kbps}$

VOLIAMO SAPERE SE UTILIZZANDO UNO
DROP TAIL IL BUFF SI
INIZIA A DROPPARE SE SI QUANDO

$S_1 \rightarrow 1 \rightarrow 4$ CON 300 kbps

ports = 1520 bytes

$$1520 \times 8 = 12160 \text{ bit}$$

IL BUFFER PUO' GESTIRE

$$\text{PKT NEL BUFFER} = \frac{2000000}{1520 \cdot 8}$$

$$\approx 164,47$$

$$\approx 164 \text{ PKT}$$

$$\rightarrow 300 \cdot 1000 \times 4$$

$$\approx 1200000 \text{ bit}$$

4 PKT in 1 sec =

$$1599,687 \approx 1600 \text{ PKT}$$

Solo con S1 non si accumulano pacchetti

→ Quando parte S2 1 → 10 Sec con 150 kbps

→ Parte di accumulo è proprio 150 kbps

$$150000 \text{ bit} = \left\lfloor \frac{150000}{12160} \right\rfloor = 12,33 = 12 \text{ PKT}$$

Questa situazione è valida da 1-5

Quindi solo x 1 sec:

$$\begin{matrix} 1 \\ \downarrow \\ 12 \end{matrix} \quad \begin{matrix} 3 \\ \downarrow \\ 12 \end{matrix} \quad \begin{matrix} 4 \\ \downarrow \\ 12 \end{matrix} \Rightarrow \text{MAX QUEUE SIZE} \\ 12 \times 3 = 36$$

Sappiamo che la coda è 165 pkt
quindi non abbiamo pacchetti dropped

$$\text{MAX DELAY} = \frac{12160}{150000} \times 36 = 2,9184 \text{ Sec}$$

Cosa succederebbe se invece S2 generasse a 1 Mbps

$$\Rightarrow \frac{1000000}{12160} = 82,23 \text{ pkt} \approx 83$$

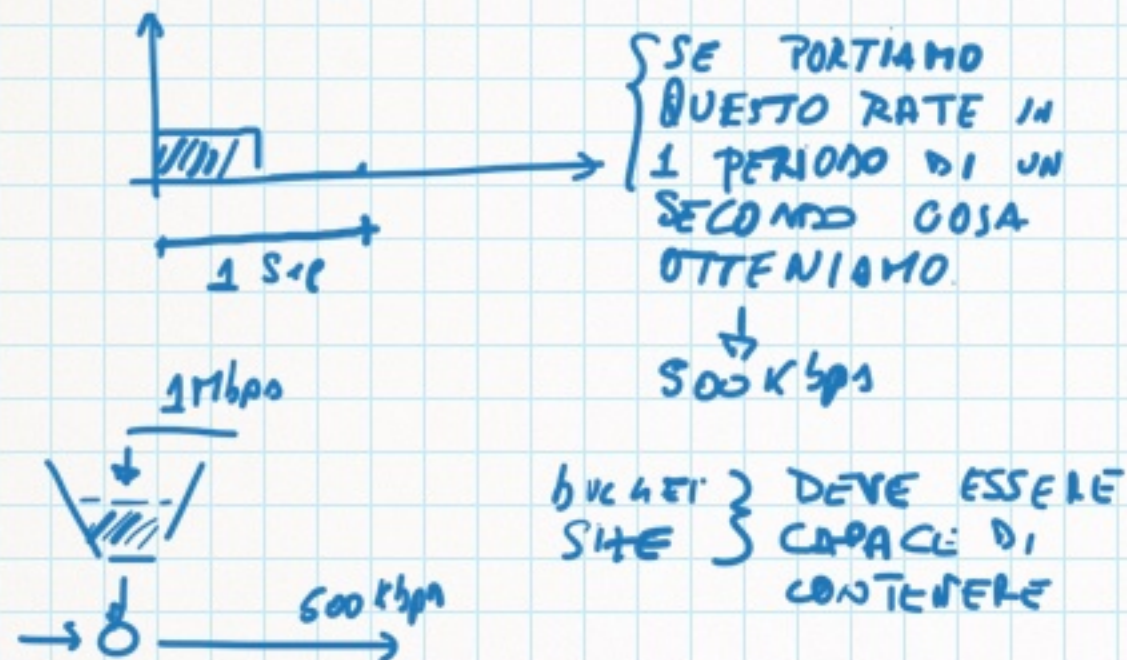
$$83 \times 3 = 249 \text{ pkt} > 165 \text{ pkt} \Rightarrow \text{DROP}$$

$$\text{MAX LATENCY} = \frac{165 \times 12160}{150000} = 13,29 \text{ ms}$$

$$(82 \times 3) \leq 165 = \frac{81}{165} = 2$$

$$\begin{aligned} 150000 \times x &= 200000 \\ x &= \left(\frac{150000}{200000} \right)^{-1} = \left(\frac{150}{200} \right)^{-1} \\ x &= 0,075 \text{ sec} = 75 \text{ ms} \end{aligned}$$

SUPPONIAMO ORA DI AVERE 52 MA
LIMITATA DA UN TRAFFICO BURST
1 Mbps MA SOLO IN 500 MS



$$Z \approx \frac{500000 \times 1 \text{ sec}}{12160} = 41,11$$

$$Z = 42 \Rightarrow 42 \times 12160$$

$$= \boxed{498560 \text{ bps}}$$

PER SAPERE QUANTO TEMPO HO PRIMA
CHE IL BUFFER SI RIEMPIA DEVO
SEMPLICEMENTE

$$x = \frac{2000000}{498560} = 4,011 \text{ sec.}$$

SE VOLESSIMO USARE
RED CONSIDERANDO
CHE LA MAX LATENZA
SIA 2 Sec.

$$\text{latenza} = \frac{\# \text{ pkt} \times 12160}{150000}$$

$$\frac{2 \times 150000}{12160} = \lfloor 24,67 \rfloor$$

$$= 24$$

$$24 \times 12160 = 291840 \text{ bt}$$

$$\text{MAX.Th} = 291840$$

$$\text{MIN.Th} = \frac{291840}{2}$$

$$= 145920 \text{ bt}$$

INIZIEREMO A DROPPARE
QUANDO

$$498560 \times 20 = 145920$$

$$x = 0,2927 \quad | \quad T = 4,1927$$

IN REALTA' PENSO
ANNO'

$$2-4 \Rightarrow 498560$$

$$4 \rightarrow 10 : (498560 - 1)$$

$$548560 \frac{150000}{\text{bps}}$$

APPROCCIO BASATO SU RED $N_f = 0,03$
 $MAX.P = 0,1$

VOGLIAMO CHE $MAX.TH = 3 MIN.TH$

VOGLIAMO MINIMIZZARE LA PRESENZA DEI
 PACCHETTI ALL' INTERNO DEL BUFFER

BUFFER = 1,5 MBIT } DI QUESTI 0,3
 SARA' NO RISERVATI

$B = 1,5 - 0,3 = 1,2$ Mbit RISERVATI AI
 DATI

$MAX.TH = 1,2 \Rightarrow \frac{12000}{8} = 1500 \text{ Bytes}$

$MIN.TH = \frac{1,2}{3} \Rightarrow \frac{12000}{24} = 500 \text{ Bytes}$

$\phi_{CHT} =$
 1 KByte

$MAX.TH = 150 \text{ pacchetti}$

$MIN.TH = 50 \text{ pacchetti}$

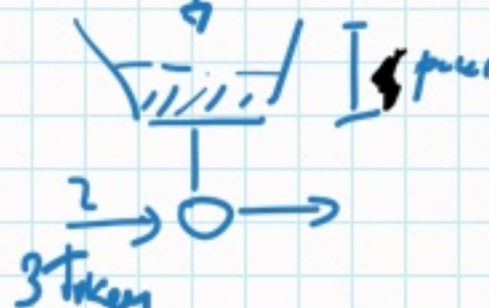
$$\frac{500 \text{ kbps}}{1000 \cdot 8} = \frac{400000 \cdot 0,08}{1000 \cdot 8} = 4$$

$R_m = 4 \text{ pacchetti ogni } 80 \text{ ms}$

$R_{on} = 40 \text{ pacchetti/sec}$

$$R_{out} = \frac{4 \cdot 8000}{0,1} = \frac{32000}{0,1} = 320 \text{ kbps} = 4 \text{ Token}$$

500 kbps per 80 ms ON
 10 ms OFF



40 Token/sec $\Rightarrow 40 \cdot 0,1$

$= 4 \text{ Token}$

DATO CHE USCIRANNO
 40 pacchetti AL SECONDO
 CALCOLIAMO DOPO
 QUANTO TEMPO
 RAGGIUNGEREMO LA
 $MIN.TH = 50$

$$50 = 40x$$

$$x = \frac{50}{40} = \frac{5}{4} = 1,25$$

$$\Delta w = (1 - N_f) \cdot w_f + N_f \cdot q$$

$$= (1 - 0,03) \cdot 40 + 0,03 \cdot 40$$

$$= 40$$

$$p_h = \frac{MAX.P \cdot (MAX.TH - MIN.TH)}{MAX.TH \cdot MIN.TH}$$

$$\Delta w_{go} = \frac{MAX - MIN.TH}{2} \cdot MIN.TH$$

$$\phi_a = \frac{p_h}{1 - (e_{as} \cdot P_0)}$$

Suppongo un drop
 ogni 2 pacchetti in
 arrivo $\Rightarrow$ ottengo
 38 pacchetti
 ogni 100 ms arrivano
 2 pacchetti

PER ARRIVARE A 150 e PARTIRE DA
 50 $\Rightarrow 150 - 50 = 100$ pacchetti NE
 RIMANGONO 2 ogni 100 ms si

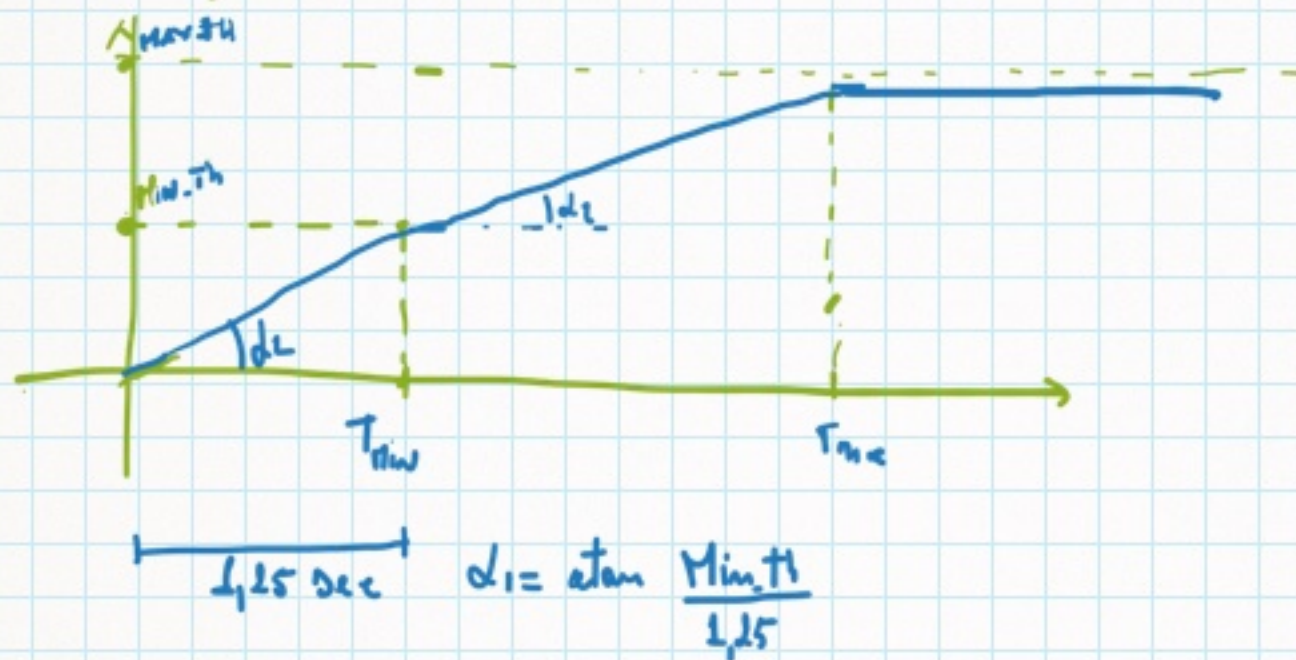
$$R_{out} \geq 20 \text{ pkts/s} = 20 \cdot 1000 \cdot 8$$

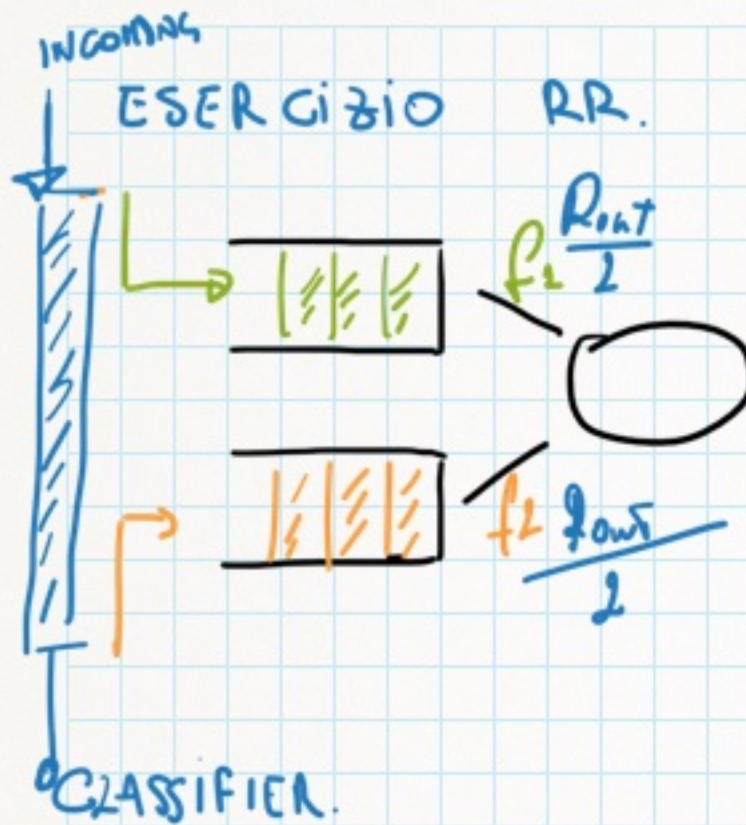
$$\quad \quad \quad \downarrow$$

$$\quad \quad \quad 20000 \cdot 8 = 160 \text{ Kbps}$$

NON RIMARRANNO pacchetti nel Buffer
 SI INVECE

CHE IL Buff. SI RIEMPIRA' FINO
 A RAGGIUNGERE IL MAX-TH,
 $R_{out} < 160 \text{ Kbps} \Rightarrow$ otturamento





$$R_{out} = 500 \text{ kbps}$$

$$R_{f1}$$

$$R_{f2}$$

$$R_{f1} + R_{f2} = R_{out}$$

$$\sum_{i=1}^n f_i = R_{out}$$

RR

RITARDO MEDIO f_1
RITARDO MEDIO f_2

$$R_{in}(f_1) = 400 \text{ kbps}$$

$$R_{in}(f_2) = 150 \text{ kbps}$$

$$R_{f1} = \frac{500}{2} = 250 \text{ kbps}$$

$$R_{f2} = \frac{500}{2} = 250 \text{ kbps}$$

$$P_{pkts} = 1536 \text{ Bps}$$

$$= 12288 \text{ bps}$$

CALCOLIAMO QUANTI
PKTS/SEC ARRIVANO
DA f_1

$$\left\lfloor \frac{400000}{12288} \right\rfloor = \left\lfloor 32,5 \right\rfloor$$

$$= 32 \text{ } f_1$$

PACCHETTI DA f_2

$$\left\lfloor \frac{150000}{12288} \right\rfloor = \left\lfloor 12,20 \right\rfloor$$

$$= 12 \text{ } f_2$$

QUANTI PACCHETTI RIMANGONO NEL BUFFER
 f_1

$$400000 - 250000 = 150 \text{ kbps}$$

$$\left\lfloor \frac{150000}{12288} \right\rfloor = 12$$

$$\left\lfloor \frac{245760}{12288} \right\rfloor = 20 \text{ pkts}$$

$$245760 \text{ bps}$$

CONSIDERIAMO PKTS

$$393216 - 245760$$

$$147456 \text{ bps} \approx 32 - 20 = 12 \text{ pkts/sec}$$

CONSIDERANDO
RATE
EQUIVALENTI

$$\frac{147456}{12288} = 12 \text{ pkts/sec}$$

DALL' ANALISI RISULTA
CHE NEL BUFFER DI
 f_1 SI ACCUMULANO

12 PACCHETTI AL SECONDO
SUL BUFFER DI f_2
NON SI ACCUMULANO PKTS

SUPPONENDO UN BUFFER (F_1, F_2)
 PARI A 2 Mbit INDICARE QUANDO
 IL FLUSSO F_2 SATURERA' IL BUFFER

→ SA PIAMO CHE RIMANGONO 12 pkts/mc

$$2 \text{ Mbit} \Rightarrow \left\lfloor \frac{2000000}{12 \cdot 288} \right\rfloor = \left\lfloor 162,76 \right\rfloor = 162$$

$$T_{\text{tot}} = \frac{162}{12} = 13,5 \text{ sec.}$$

DA UNA SUCCESSIVA OSSERVAZIONE E'
 EMERSO CHE IL BUFFER RELATIVO
 AL FLUSSO F_1 E' OCCUPATO AL
 50% - QUALE SARA' LA LATENZA
 MEDIA

SE IL BUFFER E' OCCUPATO AL 50%

$$B = \frac{1000000}{12288} = 81 \text{ PACCHETTI}$$

$$\frac{81 \cdot 12288}{150000} = 3,98 \text{ second}$$

CONSIDERIAMO ORA LA POSSIBILITA'
 DI UTILIZZARE UNA WFO RICALCOLARE
 I PESI AFFINCHE' SI MASSIMIZZI IL
 RATE DI F_1 EVITANDO CHE IL
 FORMARSI DI CODE PER F_2

FORMULA GENERALE E'
 LA SEGUENTE

$$R_i = \frac{W_i \cdot R}{\sum_{i=1}^n W_i}$$

$$R_{f2} = \frac{W_2 \cdot 500 \text{ kbps}}{W_1 + W_2}$$

DATO CHE R_{f2} O/E/C E' ESSERE

$$R_{f2} = 150 \text{ kbps}$$

$$150 = \frac{W_2 \cdot 500}{W_1 + W_2}$$

$$150 W_1 = (500 - 150) W_2$$

$$W_1 = \frac{350}{150} W_2$$

$$= 2,33 W_2$$

$$R_{f1} = \frac{W_1 \cdot 500}{W_1 + W_2}$$

$$= \frac{2,33 W_2 \cdot 500}{3,33 W_2}$$

$$= \frac{1165 W_2}{3,33 W_2} = 349,85 \text{ kbps}$$

①

ESERCIZI RSA

$$p = 11$$

$$q = 13$$

→ NUMERI PRIMI

$$m = p \times q = 11 \times 13 = 143$$

$$\phi(m) = (p-1) \cdot (q-1) = 10 \times 12 = 120$$

$$120 = 2 \cdot 2 \cdot 5 \cdot 2 \cdot 3 = 2^3 \times 3 \times 5 \rightarrow \text{FATTORI DI } \phi(m)$$

$$e = [3, \phi(m)] \Rightarrow 7$$

→ SCELTA DELL'ESPOONENTE PUB.
NON DEVE ESSERE UN FATTORE DI $\phi(m)$

$$e \cdot d \bmod \phi(m) \equiv 1$$

PER TROVARE LA
CHIAVE PRIVATA
D'ANDRÉ HO AD
UTILIZZARE IL METODO
EUCLIDEO ESTESO

$$a = e \quad b = \phi(m)$$

$$ax + by = \gcd(a, b) \Rightarrow e \cdot d \equiv 1 \pmod{\phi(m)}$$

$$1x + 120y = 1 \Rightarrow \text{Applico il metodo di Steiner}$$

$$x = d$$

While $a \neq 0$

$$x = 0$$

$$y = 1$$

$$u = 1$$

$$v = 0$$

$$q = b/a$$

$$r = b \% a$$

$$m = x - u \cdot q$$

$$n = y - v \cdot q$$

$$b = a$$

$$a = r$$

$$x = u$$

$$y = v$$

$$u = m$$

$$v = n$$

ESSENDO $a = 0$ RETURN b, x, y (1, -17, 1)

②

$$g, u, y = \text{egcd}(7, 120)$$

$$g = 1$$

$$u = -17$$

$$y = 1$$

if $j \neq 1$

ERROR

ELSE

$$x \cdot e \bmod \phi(m)$$

$$-17 \cdot 120$$

$$\equiv 103$$

$$q = \frac{120}{7}$$

$$r = 120 \% 7 = 1$$

$$m = 0 - 1 \cdot 17$$

$$n = 1 - 0 \cdot 17$$

$$b = 7$$

$$a = 1$$

$$x = 1$$

$$y = 0$$

$$u = -17$$

$$v = 1$$

$$q = 7$$

$$r = 0$$

$$m = 1 - (-17 \cdot 1)$$

$$= 120$$

$$n = 0 - 7$$

$$= -7$$

$$b = 1$$

$$a = 0$$

$$x = -17$$

$$y = 1$$

$$u = 120$$

$$v = -7$$

$$p = 61 \quad q = 53 \quad n = p \times q = 3233$$

$$\phi(n) = 3120$$

$$\phi(n) = 2^4 \cdot 3 \cdot 5 \cdot 13$$

$$= 2^4 \cdot 5 \cdot 3 \cdot 13$$

POSSIAMO QUINDI SCEGLIERE

$$g, x, y = \text{egcd}(e, \phi(n))$$

$$= \text{egcd}(17, 3120)$$

$$x = 0$$

$$y = 1$$

$$u = 1$$

$$v = 0$$

$$b = 3120$$

$$a = 17$$

$$q = \lfloor 3120 / 17 \rfloor = 183$$

$$r = 3120 \% 17 = 9$$

$$m = x - u \cdot q = 0 - 1 \cdot 183 = -183$$

$$n = y - v \cdot q = 1 - 0 \cdot 183 = 1$$

①

$$b = 9$$

$$a = 8$$

$$x = 1$$

$$y = 0$$

$$u = -183$$

$$v = 1$$

STEP 1 → 2

$$q = \lfloor b/a \rfloor = \lfloor 9/8 \rfloor = 1$$

$$r = b \% a = 1$$

$$m = 1 - (-183) \cdot 1 = 184$$

②

$$b = 8$$

$$a = 1$$

$$x = -183$$

$$y = 1$$

STEP 2 → 3

$$q = \lfloor b/a \rfloor = \lfloor 8/1 \rfloor = 8$$

$$r = 0$$

$$m = x - u \cdot q = -183 - (184 \cdot 8) = -367$$

$$n = y - v \cdot q = 1 - (-1 \cdot 8) = 9$$

③

$$b = 1$$

$$a = 0$$

$$x = -367$$

$$y = 0$$

STEP 3 → 4

④

$$q = 8$$

$$r = 0$$

$$m = x - u \cdot q = -367 - (-1 \cdot 8) = -367$$

$$n = y - v \cdot q = 9 - (-1 \cdot 8) = 17$$

RETURN b, x, y → 1, -367, 0

STEP FINALE: RITORNO PARAMETRI
Da $\text{egcd}(e, \phi(n))$ e Calcolo π
 $x = -367$ $y = 0$
↓
ESPONENTE
CHIAVE
PRIVATA

$$d = x \text{ mod } \phi(n)$$

$$= -367 \text{ mod } 3120$$

$$= 2753$$

ENCRIPTAZIONE
CON CHIAVE
PUBBLICA
DECIFRAZIONE
CON CHIAVE
PRIVATA

$$111^4 \text{ mod } n$$

$$= 111^2 \text{ mod } 3233 = 2185$$

$$2185^{2753} \text{ mod } 3233 = 111$$

ESERCIZIO DES

DATA LA SEGUENTE CHIAVE

$K = 83182E4260A62464$

CALCOLARE I VALORI DI

C_0 E D_0

PER CALCOLARE QUESTI VALORI
DOBBIAMO EFFETTUARE LA
PERMUTAZIONE

→ IL PRIMO PASSO È PORTARE
LA CHIAVE IN BINARIO

$K =$

8	16	24
1000 1001	0001 1000	0010 1110
0100 0010 ³²	0110 0000 ⁴⁰	1010 0110 ⁴⁸
0010 0100 ⁵⁶	0110 0100 ⁶⁴	

APPLI CHIAMO LA PERMUTAZIONE
PC-1

$K(\text{PERMUTATA}) =$

57 49

0010000 1100110 0011110 1000000
0010110 0111001 0000000 1110010

LEGGERE DA SINISTRA A DESTRA
 C_0 SONO I PRIMI 28 bit e D_0
I 28 bit

$C_0 = 0010000110011000111101000000$

$D_0 = 0010110011100100000001110010$

CALCOLARE C_8 PARTENDO
DALLA CONOSCENZA DI C_0 CALCOLATO
PRECEDENTEMENTE.

PARTENDO DALLE CHIAVI
TROVATE E CONOSCENDO
LA TABELLE DEGLI SHIFT

DOBBIAMO EFFETTUARE UNO
SHIFT A SINISTRA DI
14 POSIZIONI

$C_0 =$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	1	1	1	0	1	0	0	0	0	0	0	0

16	17	18	19	20	21	22	23	24	25	26	27	28
0	0	1	0	0	0	0	0	1	1	0	0	1