Þ.×□É~ □M¯ ®A.ÎZ□K.E. É¥ÁOÆ.1.4Đ..Û,Î

MARCO ORTISI - 2018

HackInBo®

Winter 2018 Edition

CONOSCERE LA CRITTOGRAFIA ROMPENDOLA

MARCO ORTISI - 2018

HackInBo®

Winter 2018 Edition

MARCO ORTISI

NETIZEN SINCE ~1996
AMATEUR COOK

SWIFT HEAD OF PENETRATION TESTING AND VULNERABILITY ASSESSMENT

WWW.SEGFAULT.IT

WWW.SEGFAULT.IT/CONTACT/
MARCO.ORTISI@GMAIL.COM

ENCRYPTION / DECRYPTION

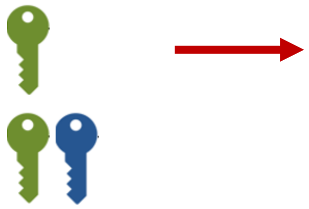
ENCRYPTION / DECRYPTION

ENCRYPTION / DECRYPTION

🔑

🔑🔑

ENCRYPTION / DECRYPTION



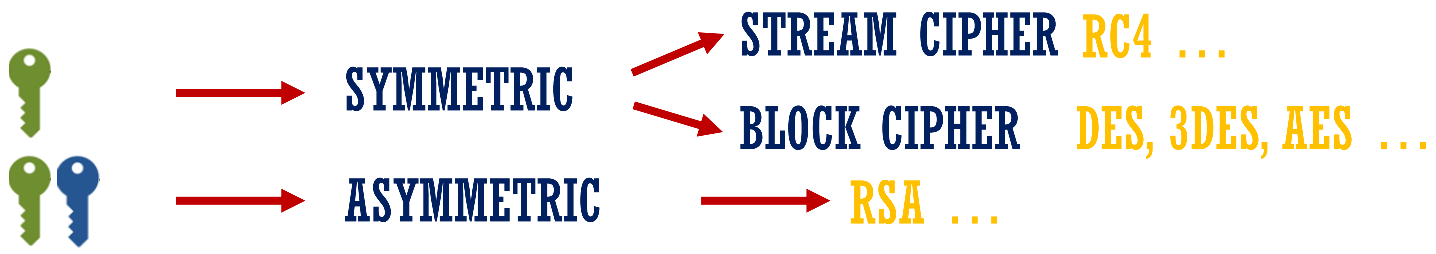
SYMMETRIC

ENCRYPTION / DECRYPTION

🔑 → SYMMETRIC

🔑🔑 → ASYMMETRIC

ENCRYPTION / DECRYPTION



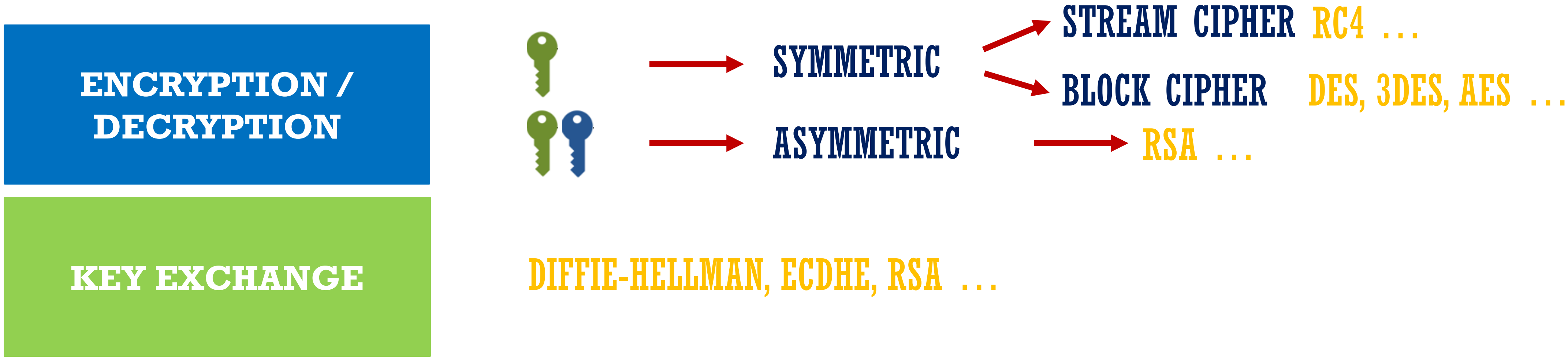
SYMMETRIC

STREAM CIPHER RC4 …

BLOCK CIPHER DES, 3DES, AES …

ASYMMETRIC

RSA …



ENCRYPTION / DECRYPTION

SYMMETRIC → STREAM CIPHER RC4 …

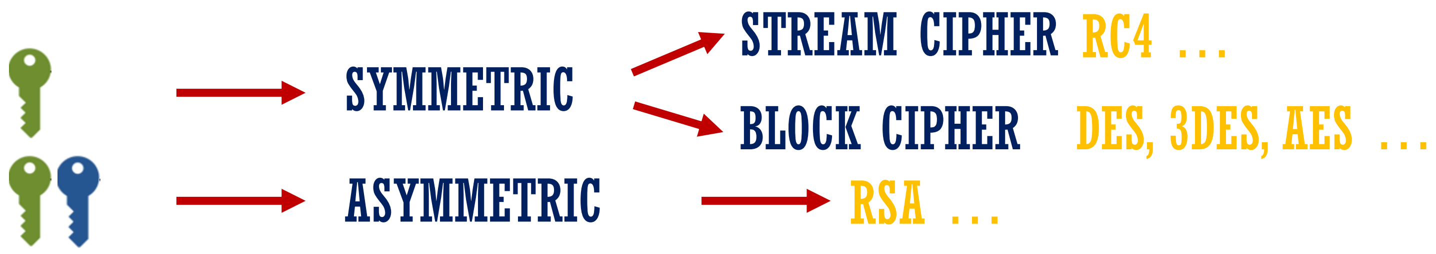
SYMMETRIC → BLOCK CIPHER DES, 3DES, AES …

ASYMMETRIC → RSA …

KEY EXCHANGE

DIFFIE-HELLMAN, ECDHE, RSA …

ENCRYPTION / DECRYPTION



SYMMETRIC → STREAM CIPHER RC4 …

SYMMETRIC → BLOCK CIPHER DES, 3DES, AES …

ASYMMETRIC → RSA …

KEY EXCHANGE

DIFFIE-HELLMAN, ECDHE, RSA …

AUTHENTICATION

DSA, ECDSA, RSA …

MUOVERE LE TRUPPE DAL PUNTO TANGO AL PUNTO FOXTROT ALLE ORE 11:00. ALLE ORE 15:00 BOMBARDARE IL PUNTO SALSA E LISCIO.

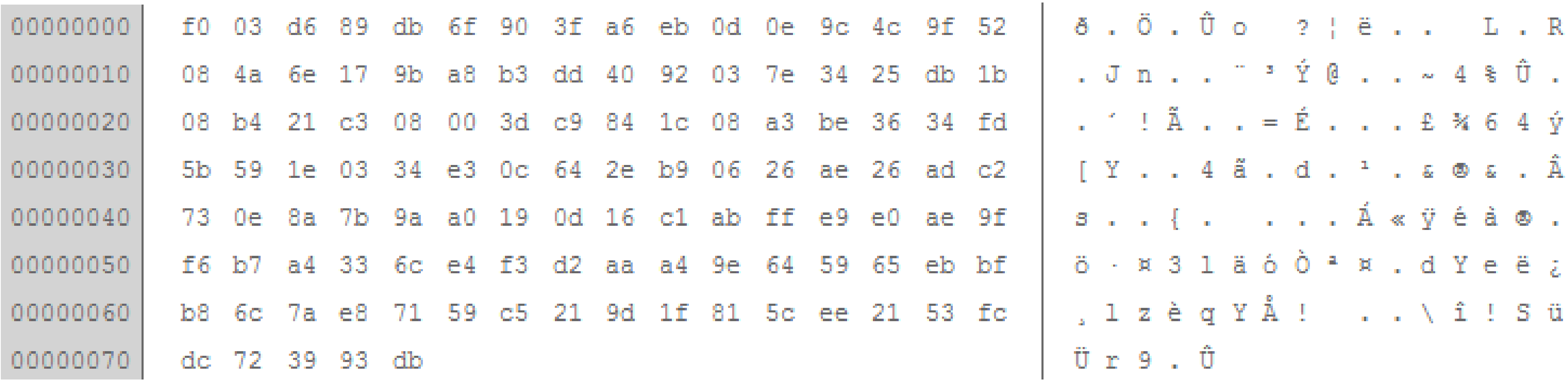
MUOVERE LE TRUPPE DAL PUNTO TANGO AL PUNTO FOXTROT ALLE ORE 11:00. ALLE ORE 15:00 BOMBARDARE IL PUNTO SALSA E LISCIO.

⬇

RC4 KEY: "HACKINBO"

MUOVERE LE TRUPPE DAL PUNTO TANGO AL PUNTO FOXTROT ALLE ORE 11:00. ALLE ORE 15:00 BOMBARDARE IL PUNTO SALSA E LISCIO.

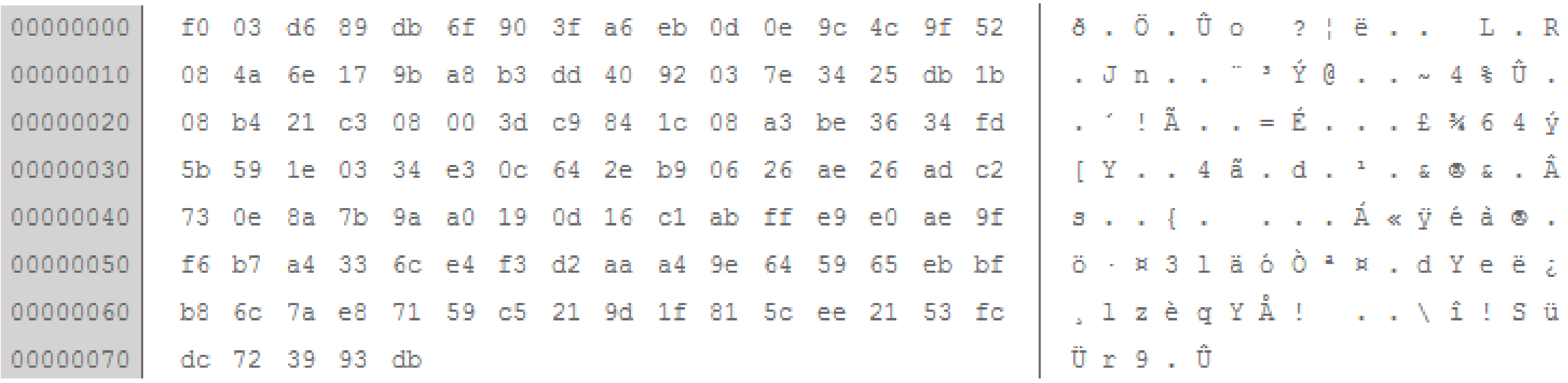
RC4 KEY: “HACKINBO”



```
00000000  f0 03 d6 89 db 6f 90 3f a6 eb 0d 0e 9c 4c 9f 52  ð . Ö . Û o   ? ¦ ë . .   L . R
00000010  08 4a 6e 17 9b a8 b3 dd 40 92 03 7e 34 25 db 1b  . J n . . ¨ ³ Ý @ . . ~ 4 % Û .
00000020  08 b4 21 c3 08 00 3d c9 84 1c 08 a3 be 36 34 fd  . ´ ! Ã . . = É . . . £ ¾ 6 4 ý
00000030  5b 59 1e 03 34 e3 0c 64 2e b9 06 26 ae 26 ad c2  [ Y . . 4 ã . d . ¹ . & ® & . Â
00000040  73 0e 8a 7b 9a a0 19 0d 16 c1 ab ff e9 e0 ae 9f  s . . { .   . . . Á « ÿ é à ® .
00000050  f6 b7 a4 33 6c e4 f3 d2 aa a4 9e 64 59 65 eb bf  ö · ¤ 3 l ä ó Ò ª ¤ . d Y e ë ¿
00000060  b8 6c 7a e8 71 59 c5 21 9d 1f 81 5c ee 21 53 fc  ¸ l z è q Y Å !   . . \ î ! S ü
00000070  dc 72 39 93 db                                   Ü r 9 . Û
```

MUOVERE LE TRUPPE DAL PUNTO TANGO AL PUNTO FOXTROT ALLE ORE 11:00. ALLE ORE 15:00 BOMBARDARE IL PUNTO SALSA E LISCIO.

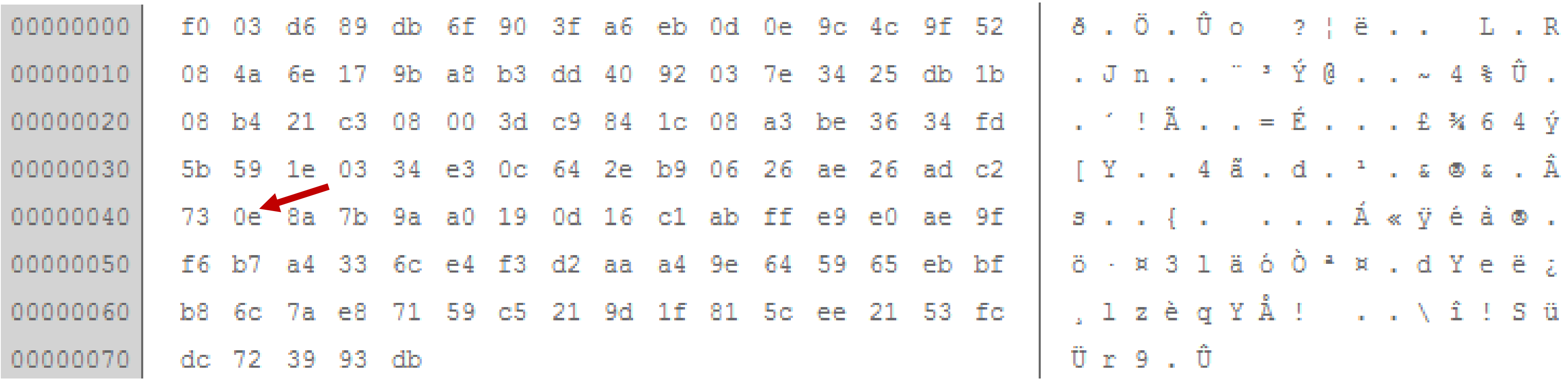
RC4 KEY: "HACKINBO"



```
00000000    f0 03 d6 89 db 6f 90 3f a6 eb 0d 0e 9c 4c 9f 52    ð . Ö . Û o   ? ¦ ë . .   L . R
00000010    08 4a 6e 17 9b a8 b3 dd 40 92 03 7e 34 25 db 1b    . J n . . ¨ ³ Ý @ . . ~ 4 % Û .
00000020    08 b4 21 c3 08 00 3d c9 84 1c 08 a3 be 36 34 fd    . ´ ! Ã . . = É . . . £ ¾ 6 4 ý
00000030    5b 59 1e 03 34 e3 0c 64 2e b9 06 26 ae 26 ad c2    [ Y . . 4 ã . d . ¹ . & ® & . Â
00000040    73 0e 8a 7b 9a a0 19 0d 16 c1 ab ff e9 e0 ae 9f    s . . { .   . . . Á « ÿ é à ® .
00000050    f6 b7 a4 33 6c e4 f3 d2 aa a4 9e 64 59 65 eb bf    ö · ¤ 3 l ä ó Ò ª ¤ . d Y e ë ¿
00000060    b8 6c 7a e8 71 59 c5 21 9d 1f 81 5c ee 21 53 fc    ¸ l z è q Y Å !   . . \ î ! S ü
00000070    dc 72 39 93 db                                     Ü r 9 . Û
```

MUOVERE LE TRUPPE DAL PUNTO TANGO AL PUNTO FOXTROT ALLE ORE 11:00. ALLE ORE 15:00 BOMBARDARE IL PUNTO SALSA E LISCIO.

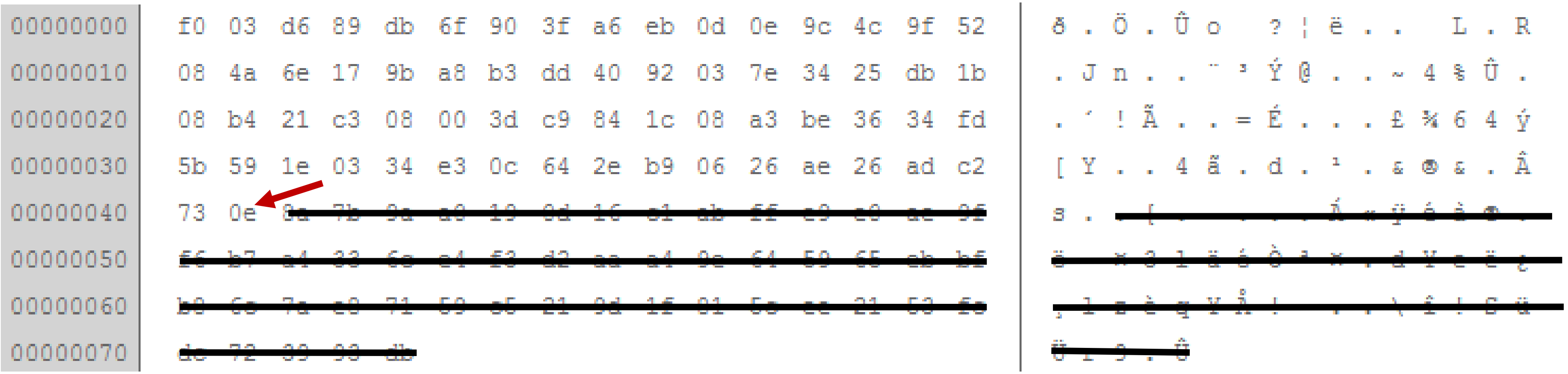
RC4 KEY: “HACKINBO”



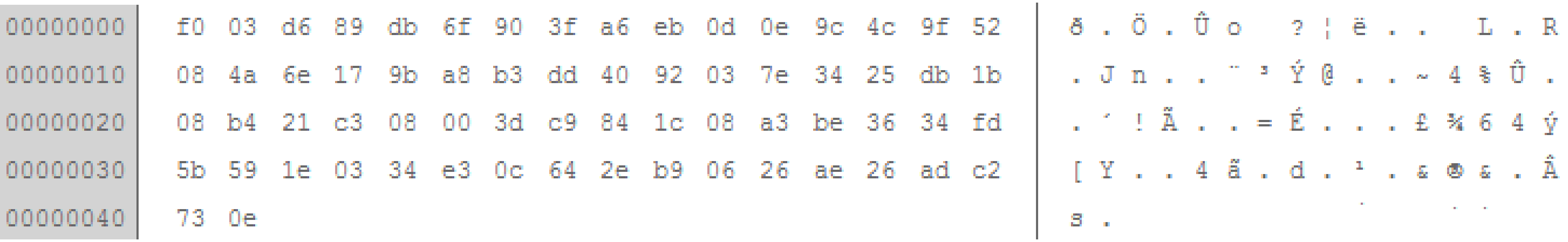
```
00000000   f0 03 d6 89 db 6f 90 3f a6 eb 0d 0e 9c 4c 9f 52   ð . Ö . Û o   ? ¦ ë . .   L . R
00000010   08 4a 6e 17 9b a8 b3 dd 40 92 03 7e 34 25 db 1b   . J n . . ¨ ³ Ý @ . . ~ 4 % Û .
00000020   08 b4 21 c3 08 00 3d c9 84 1c 08 a3 be 36 34 fd   . ´ ! Ã . . = É . . . £ ¾ 6 4 ý
00000030   5b 59 1e 03 34 e3 0c 64 2e b9 06 26 ae 26 ad c2   [ Y . . 4 ã . d . ¹ . & ® & . Â
00000040   73 0e 8a 7b 9a a0 19 0d 16 c1 ab ff e9 e0 ae 9f   s . . { .   . . . Á « ÿ é à ® .
00000050   f6 b7 a4 33 6c e4 f3 d2 aa a4 9e 64 59 65 eb bf   ö · ¤ 3 l ä ó Ò ª ¤ . d Y e ë ¿
00000060   b8 6c 7a e8 71 59 c5 21 9d 1f 81 5c ee 21 53 fc   ¸ l z è q Y Å !   . . \ î ! S ü
00000070   dc 72 39 93 db                                     Ü r 9 . Û
```

MUOVERE LE TRUPPE DAL PUNTO TANGO AL PUNTO FOXTROT ALLE ORE 11:00. ALLE ORE 15:00 BOMBARDARE IL PUNTO SALSA E LISCIO.

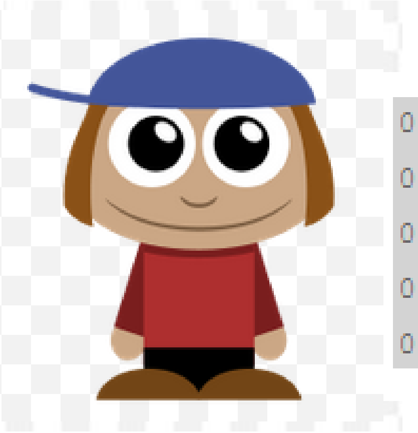
RC4 KEY: “HACKINBO”

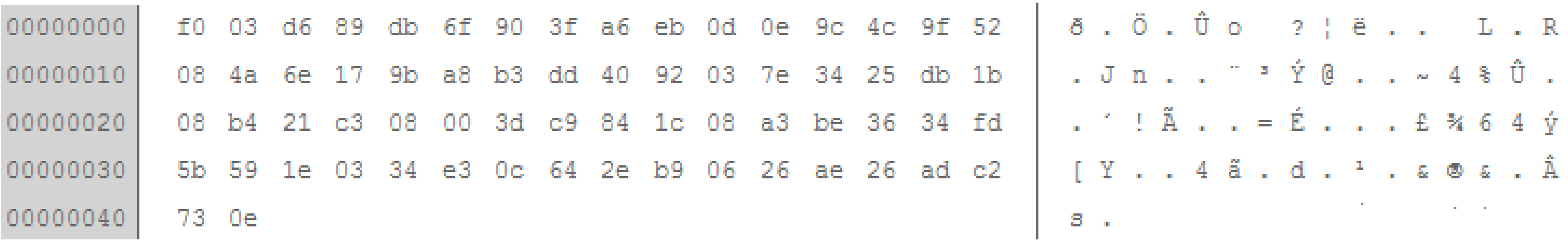


```
00000000   f0 03 d6 89 db 6f 90 3f a6 eb 0d 0e 9c 4c 9f 52   ð . Ö . Û o   ? ¦ ë . .   L . R
00000010   08 4a 6e 17 9b a8 b3 dd 40 92 03 7e 34 25 db 1b   . J n . . ¨ ³ Ý @ . . ~ 4 % Û .
00000020   08 b4 21 c3 08 00 3d c9 84 1c 08 a3 be 36 34 fd   . ´ ! Ã . . = É . . . £ ¾ 6 4 ý
00000030   5b 59 1e 03 34 e3 0c 64 2e b9 06 26 ae 26 ad c2   [ Y . . 4 ã . d . ¹ . & ® & . Â
00000040   73 0e ~~8a 7b 9a a0 19 0d 16 c1 ab ff e9 e0 ac 9f~~   s . ~~. { . . . . . Á « ÿ é à ¬ .~~
00000050   ~~f6 b7 a4 33 6c e4 f3 d2 aa a4 9e 64 59 65 eb bf~~   ~~ö · ¤ 3 l ä ó Ò ª ¤ . d Y e ë ¿~~
00000060   ~~b8 6c 7a e8 71 59 c5 21 9d 1f 81 5c ee 21 53 fc~~   ~~¸ l z è q Y Å ! . . . \ î ! S ü~~
00000070   ~~dc 72 39 93 db~~                                  ~~Ü r 9 . Û~~
```



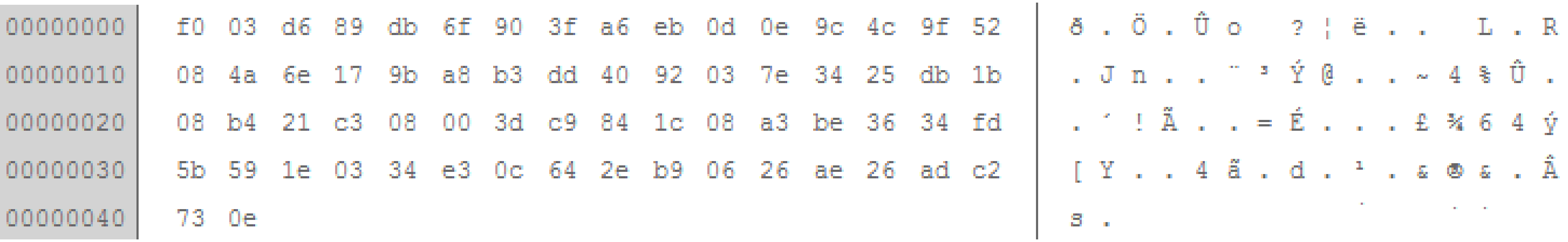
```
00000000 | f0 03 d6 89 db 6f 90 3f a6 eb 0d 0e 9c 4c 9f 52 | ð . Ö . Û o   ? ¦ ë . .   L . R
00000010 | 08 4a 6e 17 9b a8 b3 dd 40 92 03 7e 34 25 db 1b | . J n . . ¨ ³ Ý @ . . ~ 4 % Û .
00000020 | 08 b4 21 c3 08 00 3d c9 84 1c 08 a3 be 36 34 fd | . ´ ! Ã . . = É . . . £ ¾ 6 4 ý
00000030 | 5b 59 1e 03 34 e3 0c 64 2e b9 06 26 ae 26 ad c2 | [ Y . . 4 ã . d . ¹ . & ® & . Â
00000040 | 73 0e                                           | s .
```





```
00000000   f0 03 d6 89 db 6f 90 3f a6 eb 0d 0e 9c 4c 9f 52   ð . Ö . Û o   ? ¦ ë . .   L . R
00000010   08 4a 6e 17 9b a8 b3 dd 40 92 03 7e 34 25 db 1b   . J n . . ¨ ³ Ý @ . . ~ 4 % Û .
00000020   08 b4 21 c3 08 00 3d c9 84 1c 08 a3 be 36 34 fd   . ´ ! Ã . . = É . . . £ ¾ 6 4 ý
00000030   5b 59 1e 03 34 e3 0c 64 2e b9 06 26 ae 26 ad c2   [ Y . . 4 ã . d . ¹ . & ® & . Â
00000040   73 0e                                             s .
```

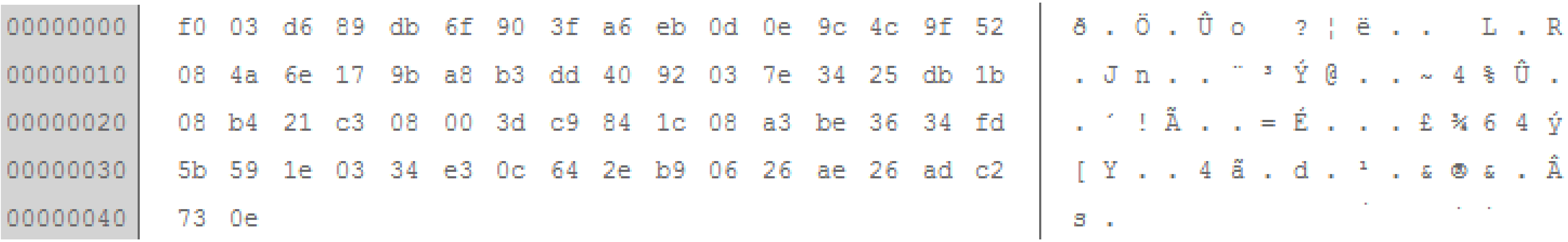
RC4 KEY: "HACKINBO"



```
00000000   f0 03 d6 89 db 6f 90 3f a6 eb 0d 0e 9c 4c 9f 52 | ð . Ö . Û o   ? ¦ ë . .   L . R
00000010   08 4a 6e 17 9b a8 b3 dd 40 92 03 7e 34 25 db 1b | . J n . . ¨ ³ Ý @ . . ~ 4 % Û .
00000020   08 b4 21 c3 08 00 3d c9 84 1c 08 a3 be 36 34 fd | . ´ ! Ã . . = É . . . £ ¾ 6 4 ý
00000030   5b 59 1e 03 34 e3 0c 64 2e b9 06 26 ae 26 ad c2 | [ Y . . 4 ã . d . ¹ . & ® & . Â
00000040   73 0e                                            | s .
```

RC4 KEY: “HACKINBO”

MUOVERE LE TRUPPE DAL PUNTO TANGO AL PUNTO FOXTROT ALLE ORE 11:00.

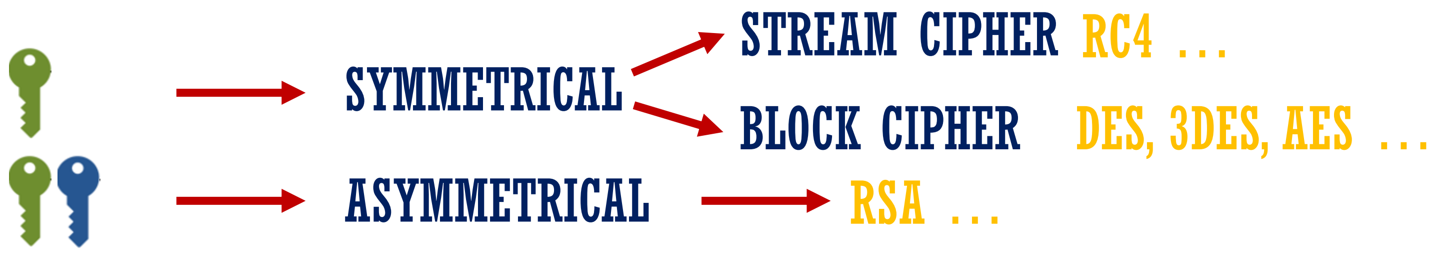


```
00000000   f0 03 d6 89 db 6f 90 3f a6 eb 0d 0e 9c 4c 9f 52 | ð . Ö . Û o   ? ¦ ë . .   L . R
00000010   08 4a 6e 17 9b a8 b3 dd 40 92 03 7e 34 25 db 1b | . J n . . ¨ ³ Ý @ . . ~ 4 % Û .
00000020   08 b4 21 c3 08 00 3d c9 84 1c 08 a3 be 36 34 fd | . ´ ! Ã . . = É . . . £ ¾ 6 4 ý
00000030   5b 59 1e 03 34 e3 0c 64 2e b9 06 26 ae 26 ad c2 | [ Y . . 4 ã . d . ¹ . & ® & . Â
00000040   73 0e                                            | s .
```

RC4 KEY: “HACKINBO”

MUOVERE LE TRUPPE DAL PUNTO TANGO AL PUNTO FOXTROT ALLE ORE 11:00. ALLE ORE 15:00 BOMBARDARE IL PUNTO SALSA E LISCIO.

ENCRYPTION / DECRYPTION



SYMMETRICAL → STREAM CIPHER RC4 …

SYMMETRICAL → BLOCK CIPHER DES, 3DES, AES …

ASYMMETRICAL → RSA …

KEY EXCHANGE

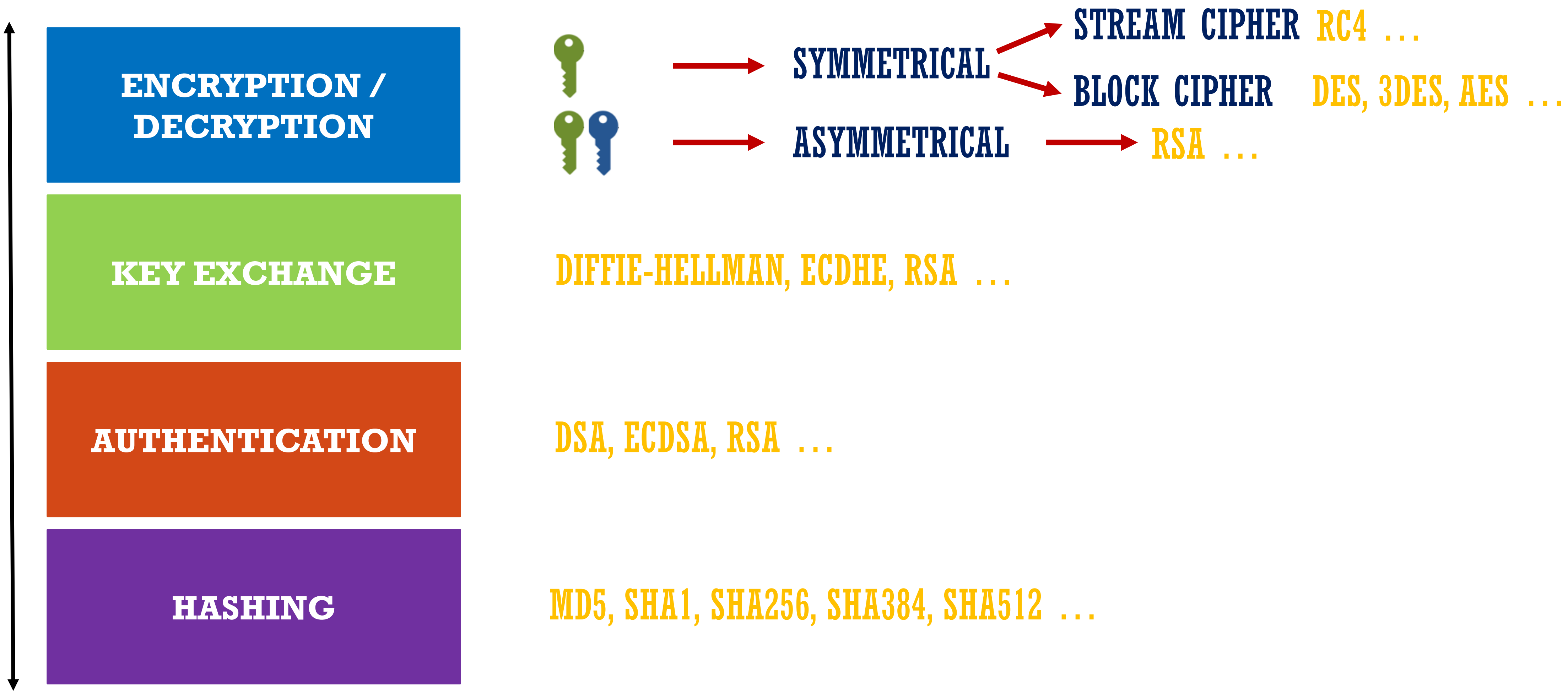
DIFFIE-HELLMAN, ECDHE, RSA …

AUTHENTICATION

DSA, ECDSA, RSA …

HASHING

MD5, SHA1, SHA256, SHA384, SHA512 …



ENCRYPTION / DECRYPTION

SYMMETRICAL → STREAM CIPHER RC4 …

SYMMETRICAL → BLOCK CIPHER DES, 3DES, AES …

ASYMMETRICAL → RSA …

KEY EXCHANGE

DIFFIE-HELLMAN, ECDHE, RSA …

AUTHENTICATION

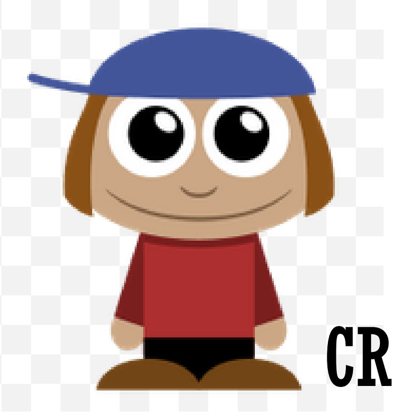
DSA, ECDSA, RSA …

HASHING

MD5, SHA1, SHA256, SHA384, SHA512 …

CRICCO

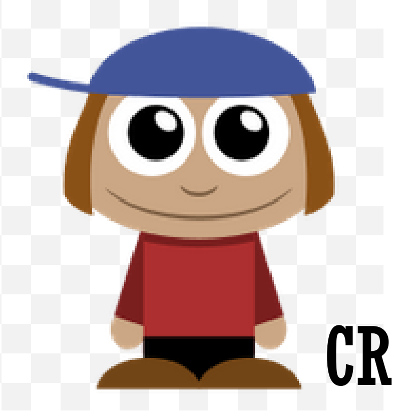
CRICCO



CROCCO

SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

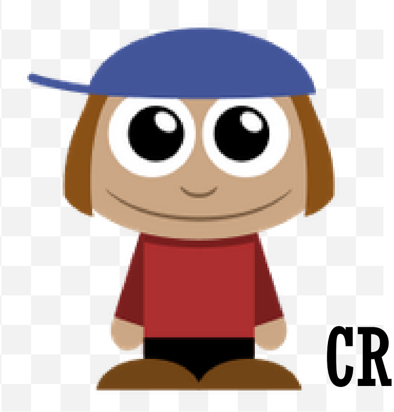
CRICCO



CROCCO

SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

CRICCO



CROCCO

n = 55

e = 3

d = 27

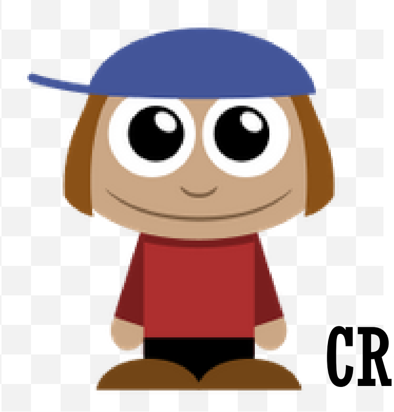
SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

CRICCO

n = 55

e = 3

d = 27



CROCCO

n = 55

e = 3

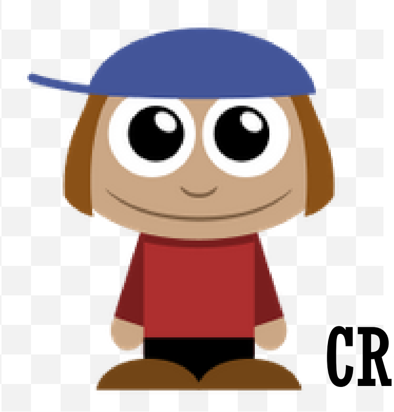
HackInBo Winter 2018 Edition

SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

$n = 55$

$e = 3$

$d = 27$



$n = 55$

$e = 3$

$m = 12$

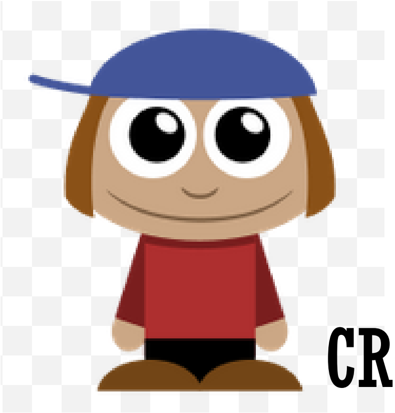
SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

CRICCO

$n = 55$

$e = 3$

$d = 27$



CROCCO

$n = 55$

$e = 3$

$m = 12$

$c = 12^3 \text{ mod } 55$

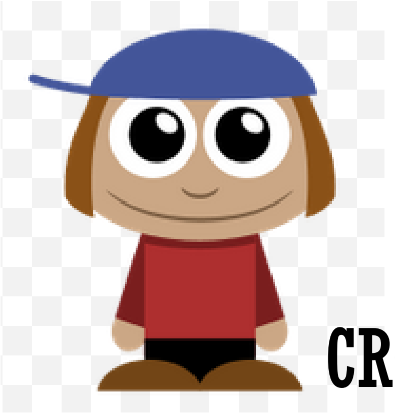
SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

CRICCO

$n = 55$

$e = 3$

$d = 27$



CROCCO

$n = 55$

$e = 3$

$m = 12$

$c = 12^3 \bmod 55$

$c = 1728 \bmod 55$

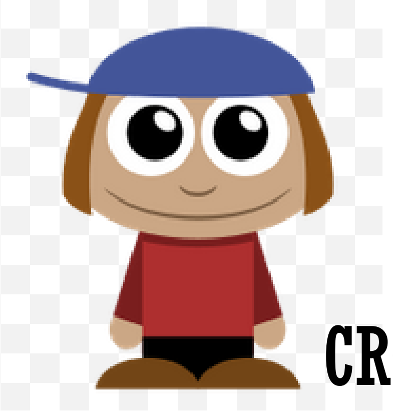
SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

CRICCO

$n = 55$

$e = 3$

$d = 27$



CROCCO

$n = 55$

$e = 3$

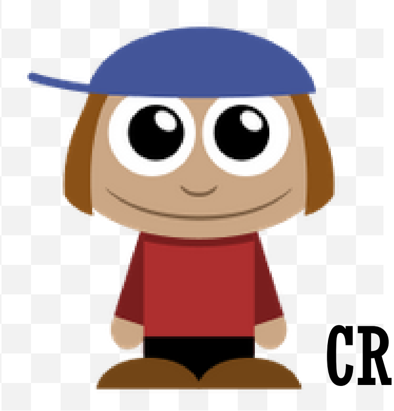
$m = 12$

$c = 12^3 \text{ mod } 55$

$c = 1728 \text{ mod } 55$

$c = 23$

SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO



CRICCO:

n = 55

e = 3

d = 27

CROCCO:

n = 55

e = 3

m = 12

$c = 12^3 \bmod 55$

$c = 1728 \bmod 55$

$c = 23$

←

c = 23

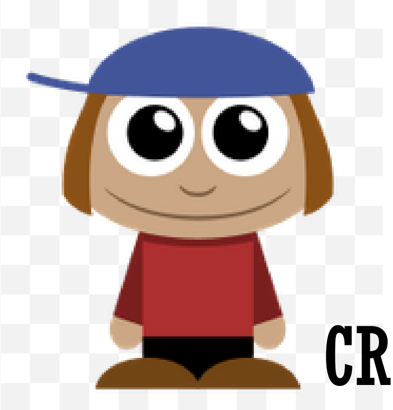
SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

CRICCO

$n = 55$

$e = 3$

$d = 27$



CROCCO

$n = 55$

$e = 3$

$m = 12$

$c = 12^3 \bmod 55$

$c = 1728 \bmod 55$

$c = 23$

$c = 23$

$m = 23^{27} \bmod 55$

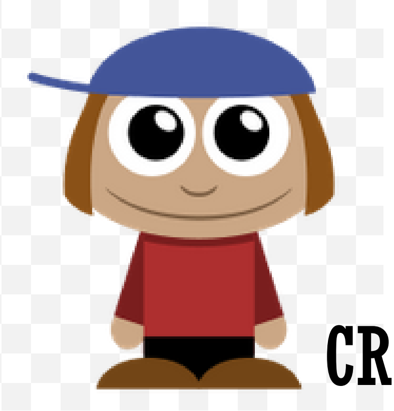
SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

CRICCO

$n = 55$

$e = 3$

$d = 27$



CROCCO

$n = 55$

$e = 3$

$m = 12$

$c = 12^3 \bmod 55$

$c = 1728 \bmod 55$

$c = 23$

$c = 23$

$m = 23^{27} \bmod 55$

$m = 58432110455545439551605946764725979847 \bmod 55$

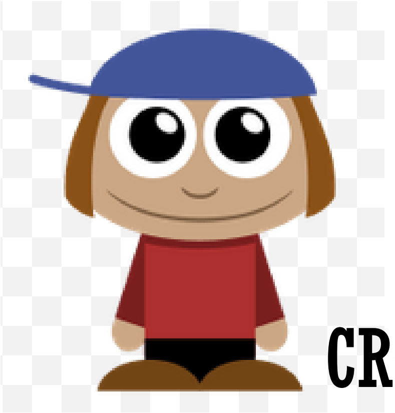
SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

CRICCO

$n = 55$

$e = 3$

$d = 27$



CROCCO

$n = 55$

$e = 3$

$m = 12$

$c = 12^3 \bmod 55$

$c = 1728 \bmod 55$

$c = 23$

$c = 23$

$m = 23^{27} \bmod 55$

$m = 5843211045545439551605946764725979847 \bmod 55$

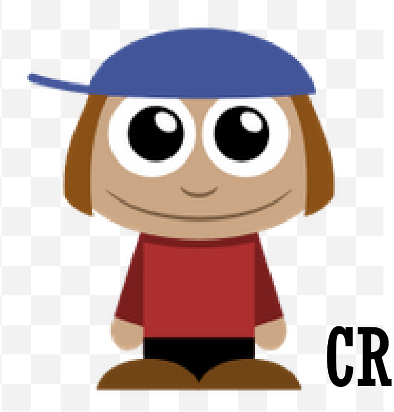
$m = 12$

SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

$n = 55$

$e = 3$

$d = 27$



$n = 55$

$e = 3$

$m = \boxed{12}$

$c = 12^3 \bmod 55$

$c = 1728 \bmod 55$

$c = 23$

$c = 23$

$m = 23^{27} \bmod 55$

$m = 5843211045545439551605946764725979847 \bmod 55$

$m = \boxed{12}$

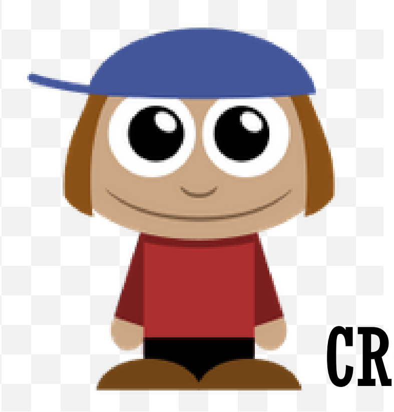
SCAMBIARSI UN NUMERO COMPRESO TRA 1 E 50 IN MODO SICURO

CRICCO

$n = 55$

$e = 3$

$d = 27$



CROCCO

$n = 55$

$e = 3$

$m = \boxed{12}$

RSA

ENCRYPTION -> $C = m^e \bmod n$

DECRYPTION -> $M = c^d \bmod n$

$c = 12^3 \bmod 55$

$c = 1728 \bmod 55$

$c = 23$

$c = 23$

$m = 23^{27} \bmod 55$

$m = 5843211045545439551605946764725979847 \bmod 55$

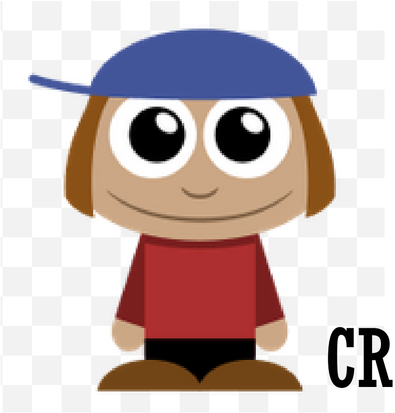
$m = \boxed{12}$

CRICCO

$n = 55$

$e = 3$

$d = 27$

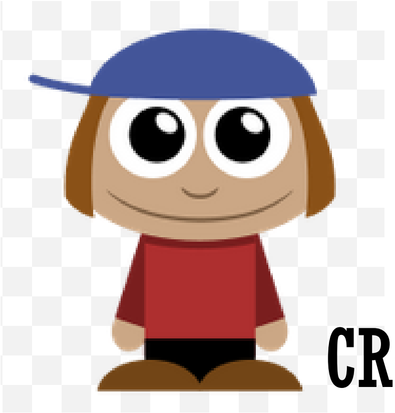


CROCCO

$n = 55$

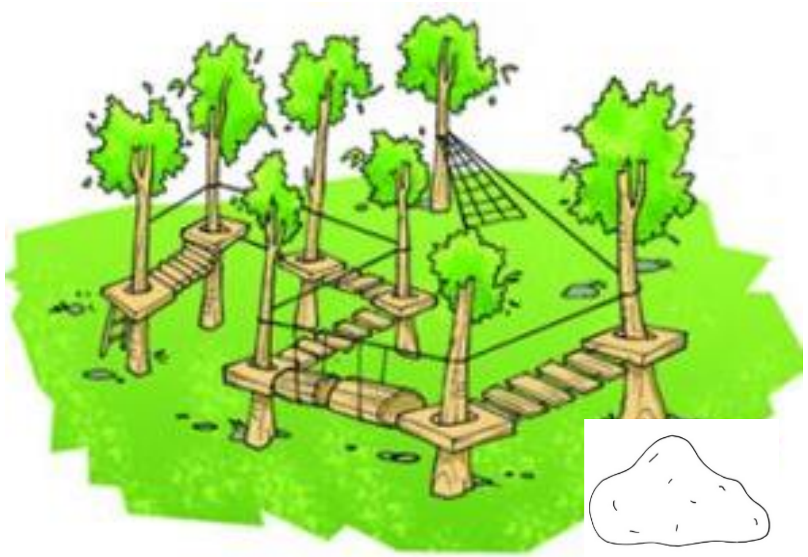
$e = 3$

CRICCO

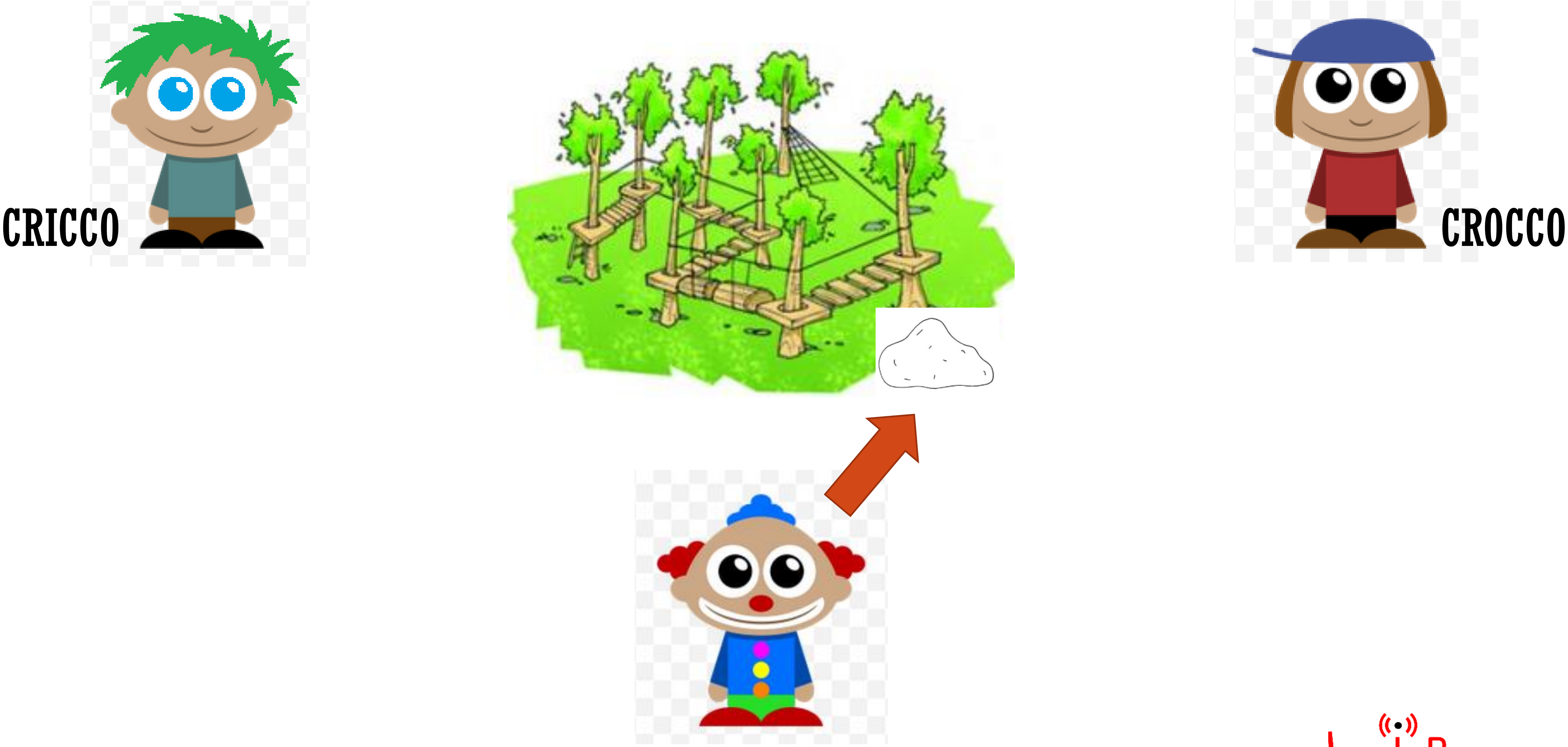


CROCCO

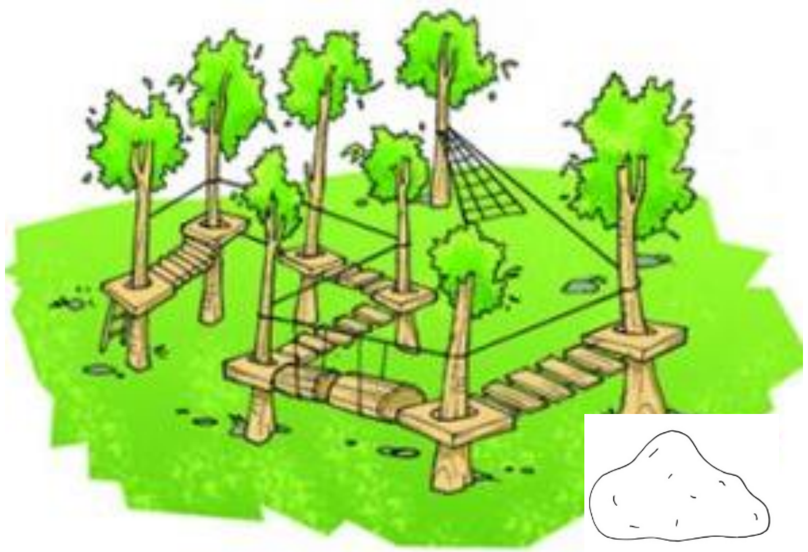
CRICCO

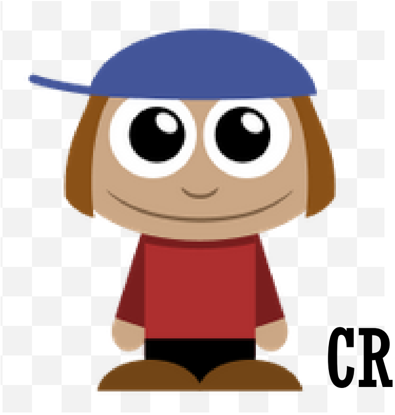


CROCCO


CRICCO
CROCCO

CRICCO





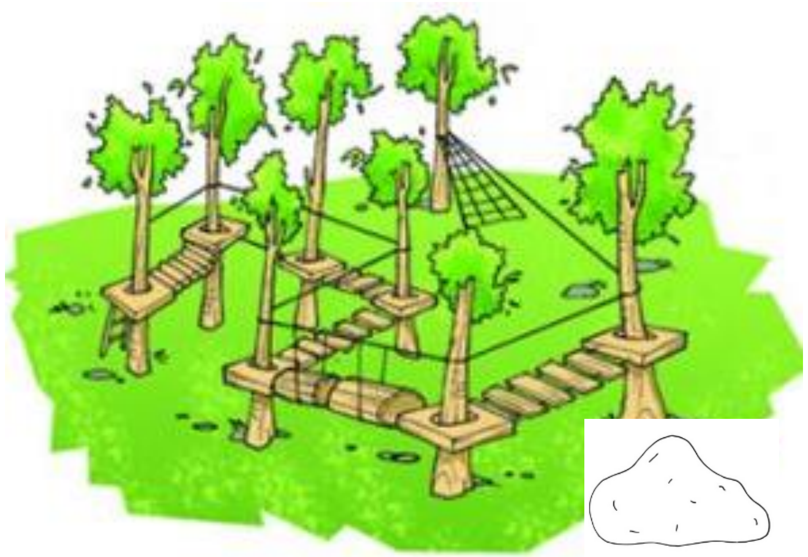
CROCCO

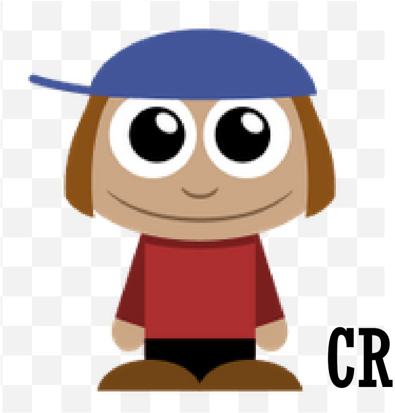
$m = 33$

CRICCO

$m = 33$

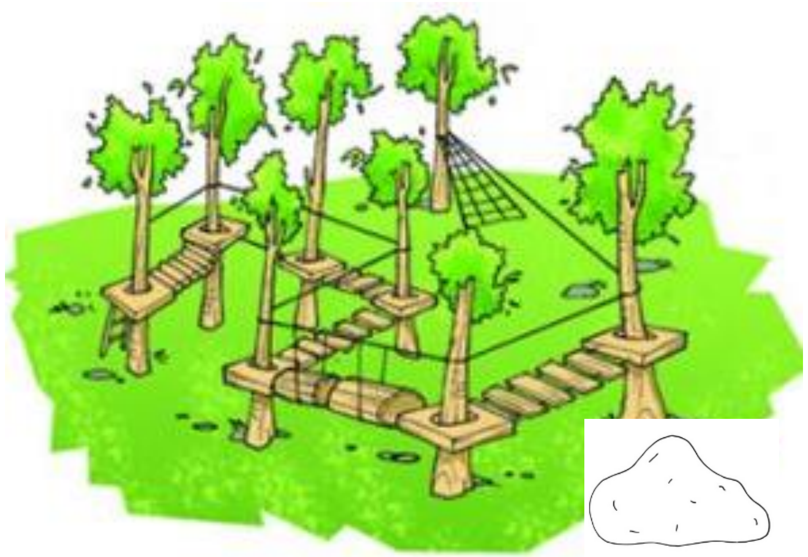
$s = 33^{27} \bmod 55$

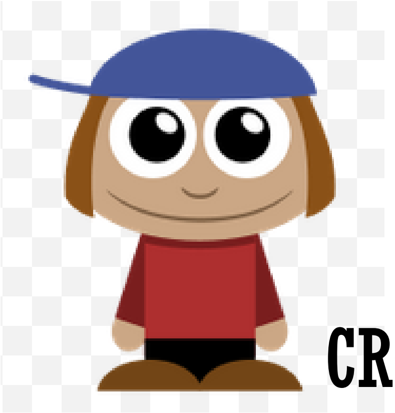




CROCCO

CRICCO





CROCCO

$\mathbf{m} = 33$

$\mathbf{s} = 33^{27} \bmod 55$

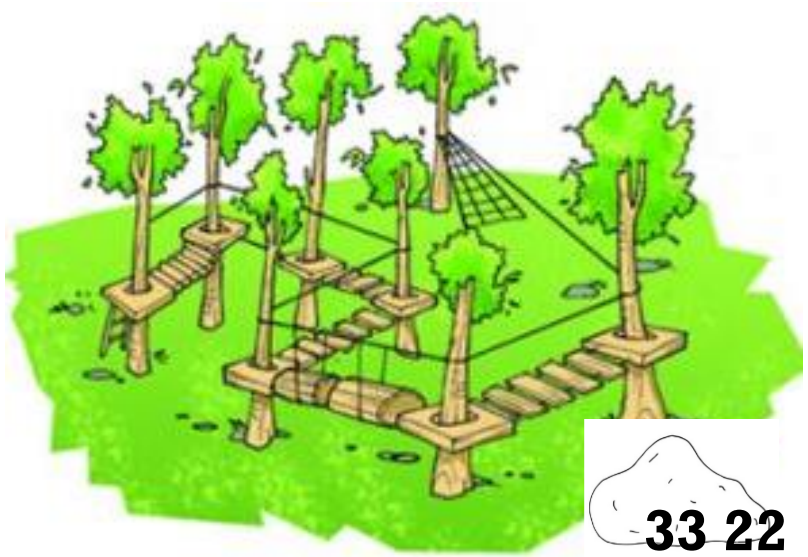
$\mathbf{s} = 22$

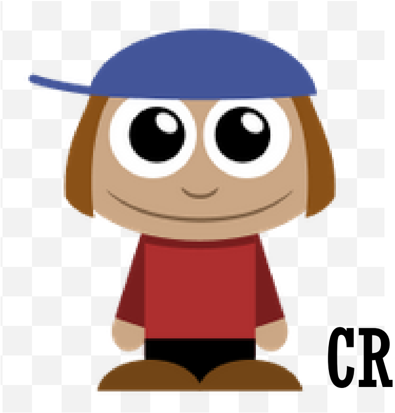
CRICCO

$\mathbf{m} = 33$

$\mathbf{s} = 33^{27} \bmod 55$

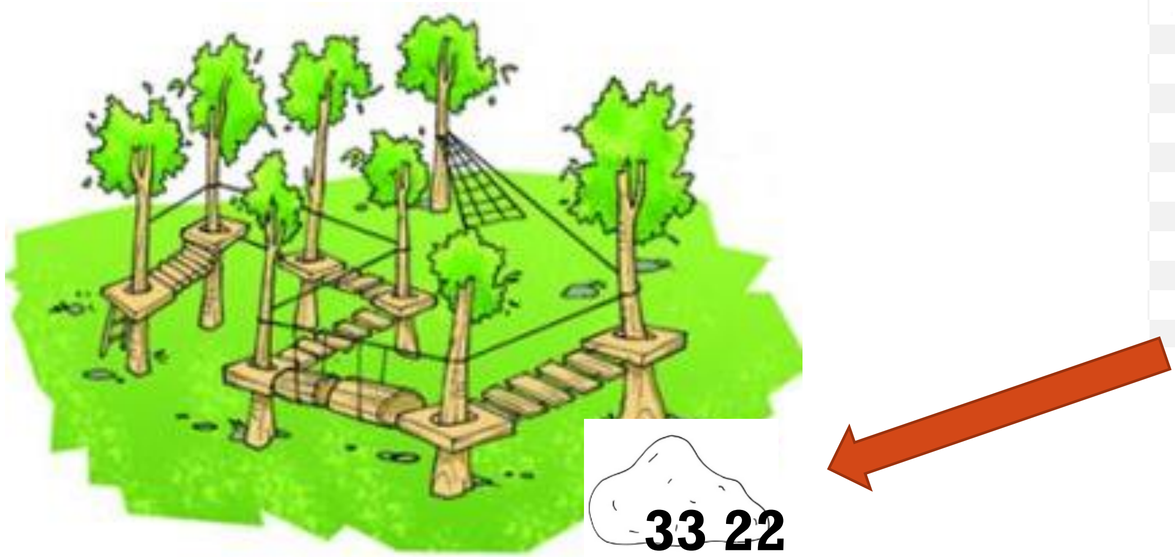
$\mathbf{s} = 22$





CROCCO

CRICCO



CROCCO

$\mathbf{m} = 33$

$\mathbf{s} = 33^{27} \bmod 55$

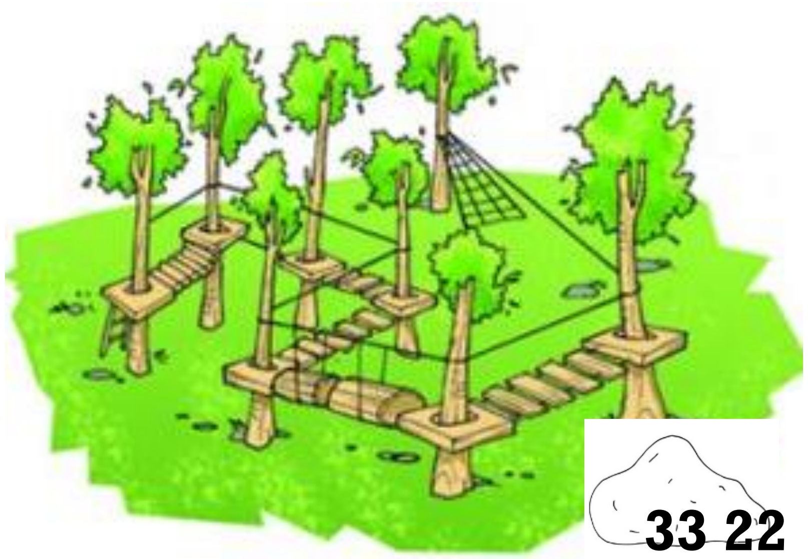
$\mathbf{s} = 22$

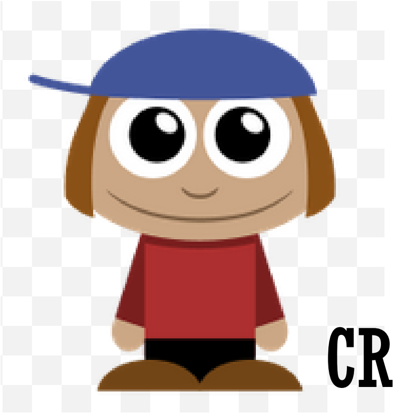
CRICCO

m = 33

s = 33^{27} **mod 55**

s = 22





CROCCO

m = 33

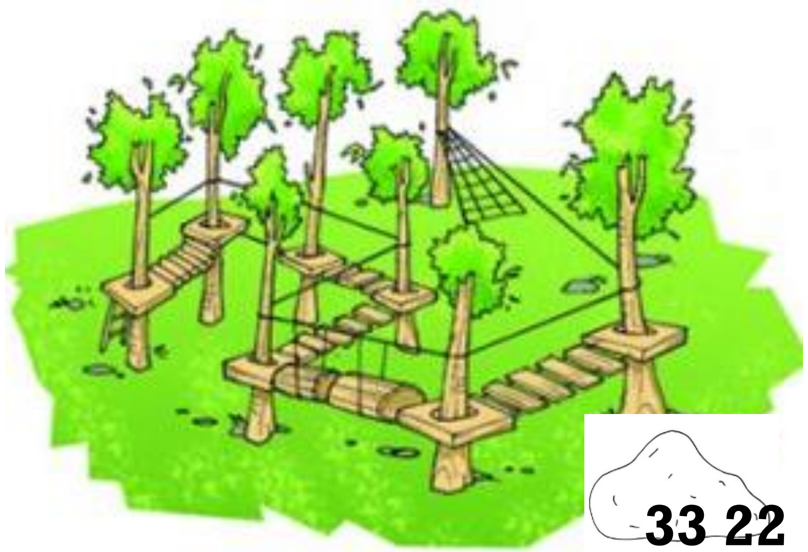
s = 22

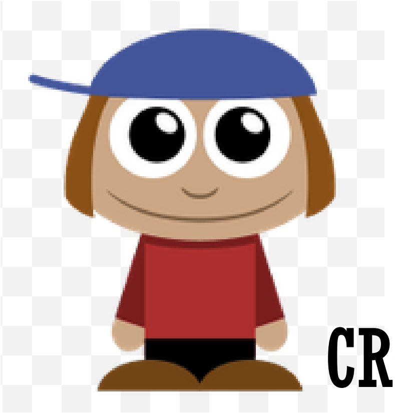
CRICCO

$\mathbf{m} = 33$

$\mathbf{s} = 33^{27} \bmod 55$

$\mathbf{s} = 22$





CROCCO

$\mathbf{m} = 33$

$\mathbf{s} = 22$

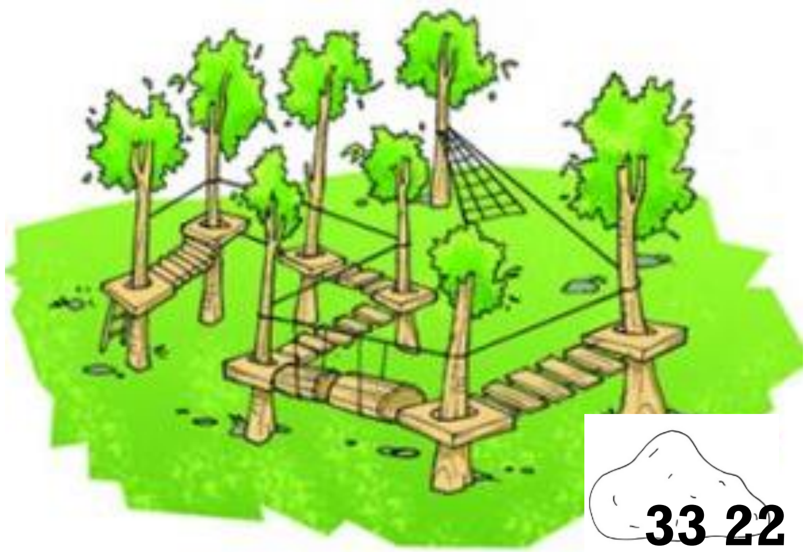
$\mathbf{ml} = 22^{3} \bmod 55$

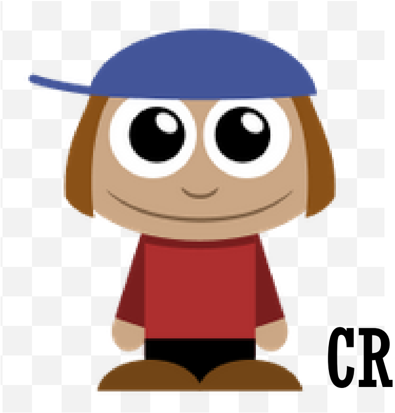
CRICCO

$\mathbf{m} = 33$

$\mathbf{s} = 33^{27} \bmod 55$

$\mathbf{s} = 22$





CROCCO

$\mathbf{m} = 33$

$\mathbf{s} = 22$

$\mathbf{ml} = 22^{3} \bmod 55$

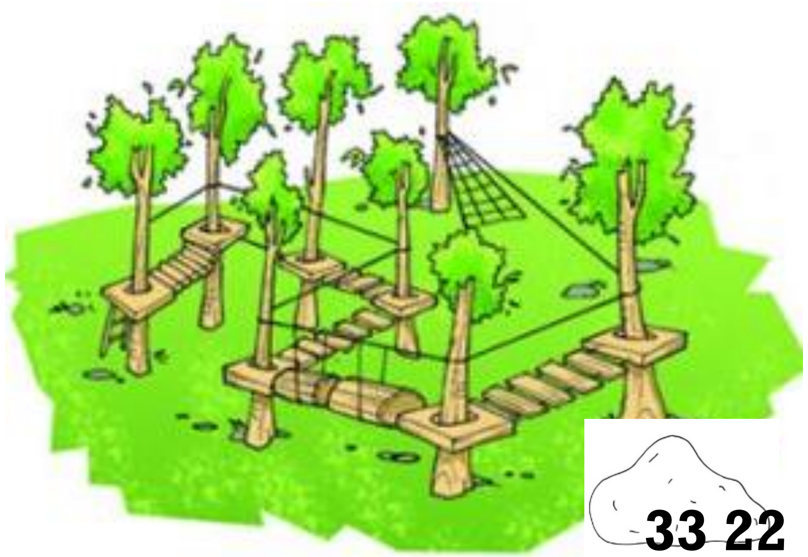
$\mathbf{ml} = 33$

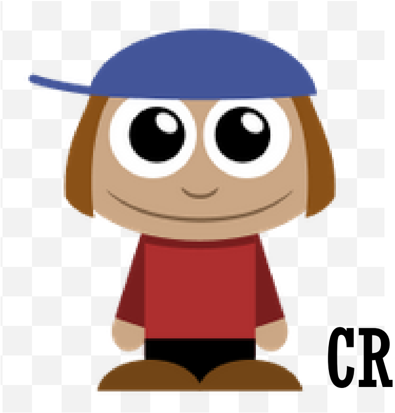
CRICCO

$m = 33$

$s = 33^{27} \bmod 55$

$s = 22$





CROCCO

$m = 33$

$s = 22$

$ml = 22^{3} \bmod 55$

$ml = 33$

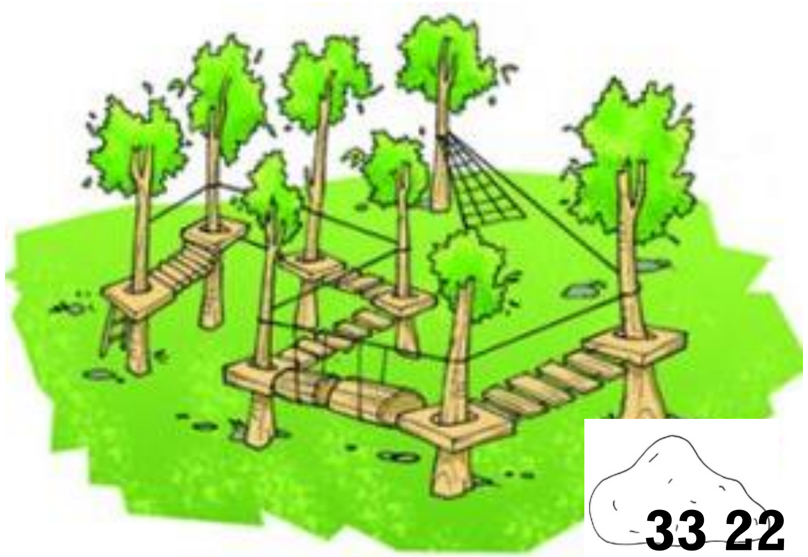
$ml == m$

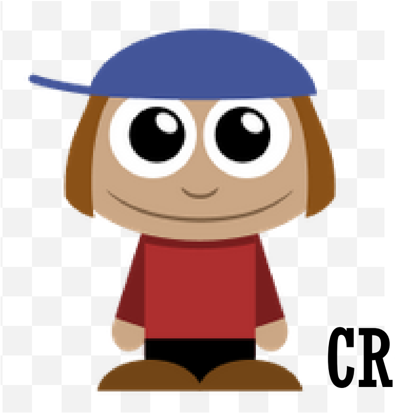
CRICCO

$m = 33$

$s = 33^{27} \bmod 55$

$s = 22$





CROCCO

$m = 33$

$s = 22$

$ml = 22^{3} \bmod 55$

$ml = 33$

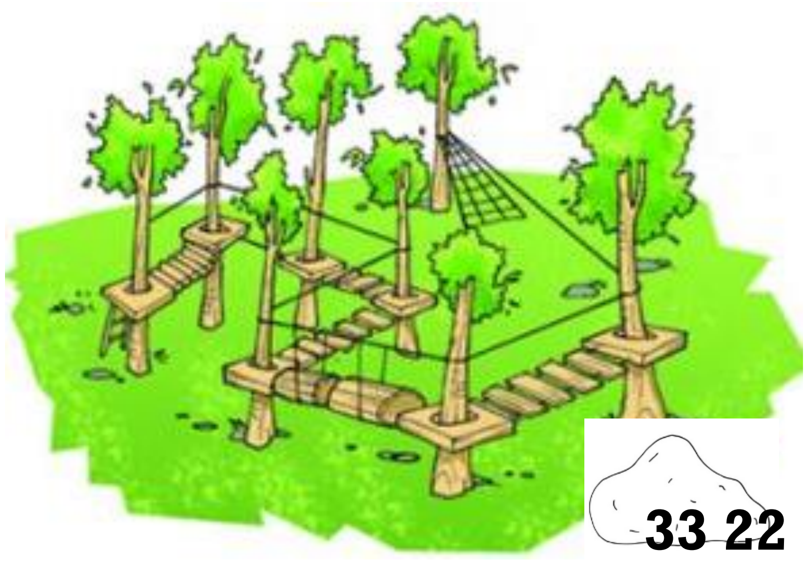
$ml == m$ **TRUE!**

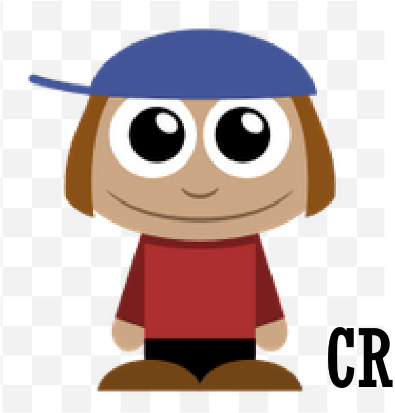
CRICCO

m = 33

s = 33^{27} **mod** 55

s = 22





CROCCO

m = 33

s = 22

ml = 22^{3} **mod** 55

ml = 33

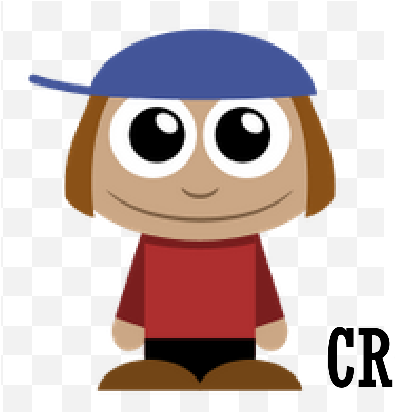
ml = = **m** **TRUE!**

CRICCO

$m = 33$

$s = 33^{27} \bmod 55$

$s = 22$



CROCCO

$m = 33$

$s = 22$

$ml = 22^{3} \bmod 55$

$ml = 33$

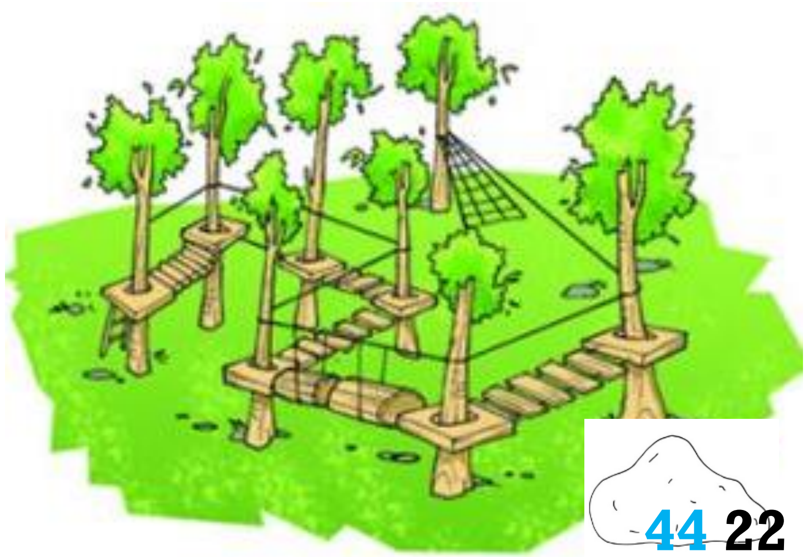
$ml == m$ **TRUE!**

CRICCO

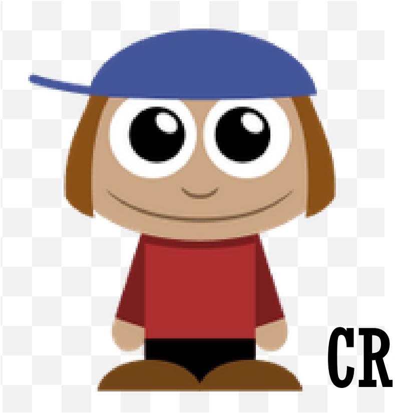
$m = 33$

$s = 33^{27} \bmod 55$

$s = 22$



CROCCO



$m = 44$

$s = 22$

$ml = 22^{3} \bmod 55$

$ml = 33$

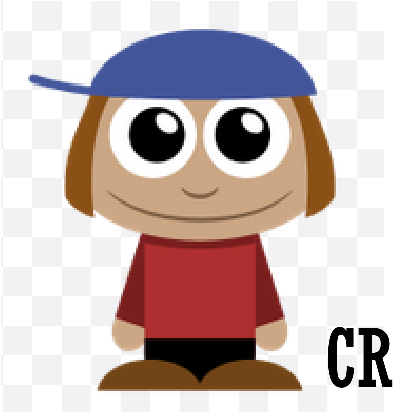
$ml == m$ **FALSE!**

CRICCO

$m = 33$

$s = 33^{\boxed{27}} \bmod 55$

$s = 22$



CROCCO

$m = 44$

$s = 22$

$ml = 22^3 \bmod 55$

$ml = 33$

$ml == m$ **FALSE!**

CRICCO

d =

10100368298420026038962070090938639792305981480825673101516457085796068778062859780752282006991706155110238664057764880668047011107282227396795611039376728858993328340937421361242786178567138008133117958457619348963458584743657819799251469649859660244233419800343280127631419344353297751507583271924732134911100093190586513439818764484885127799115426176012916806985335351691439121679102988402662117811056277000728425784848653097155900513672798427321790286986844552187927980580762303793889655383246715818082623281053372893431983230221753910171811273357314178083907334457567537612864636909811451974743817758555811413897

CRICCO

n =
227967020413111976621364875004251691313963945417526651532212021914046547338879926111913181765408081512366880644127746318263524801783226689018767076725430546968297606322972684420487129450271902620456710969947652744091395553378483499047265064036523247383106255279504614706953311144705746027672447185360460765808291787885319846234575757988012891677636699390761550646939794456827398573403755999201546325192016518960113884902731646353513736669807422650344309323417665904379586659037917393336025480792564181177770753249516358236744382000535616892253628166918568311267226309891946405795764203421072882331682934723477134576 11

e = 65537

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

$n = 55$

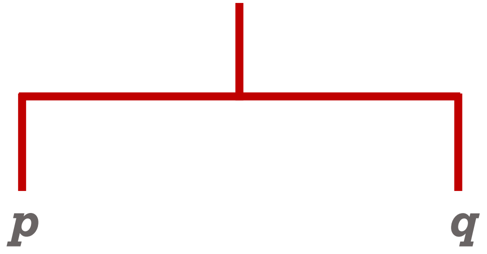
FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55

numero semiprimo, prodotto di due numeri primi

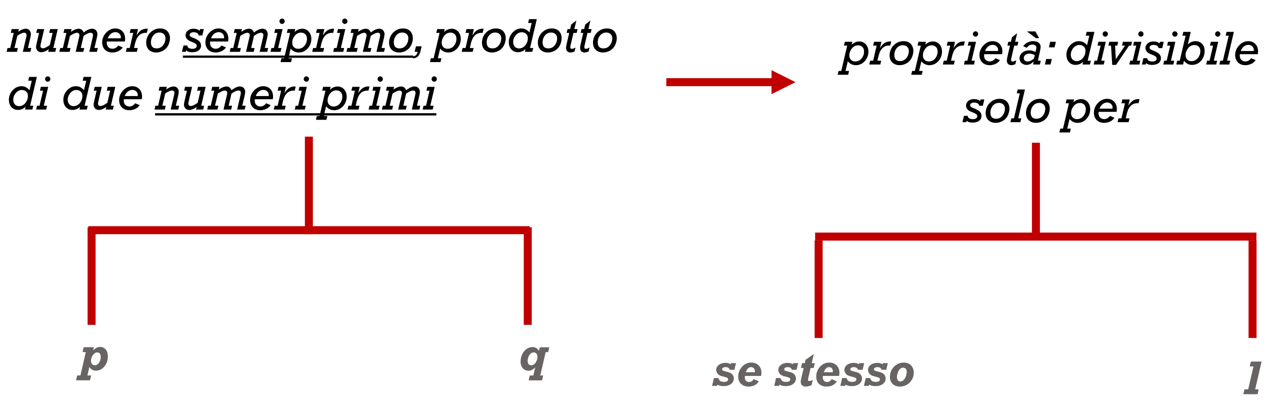


FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = **55**



numero semiprimo, prodotto di due numeri primi

proprietà: divisibile solo per

p

q

se stesso

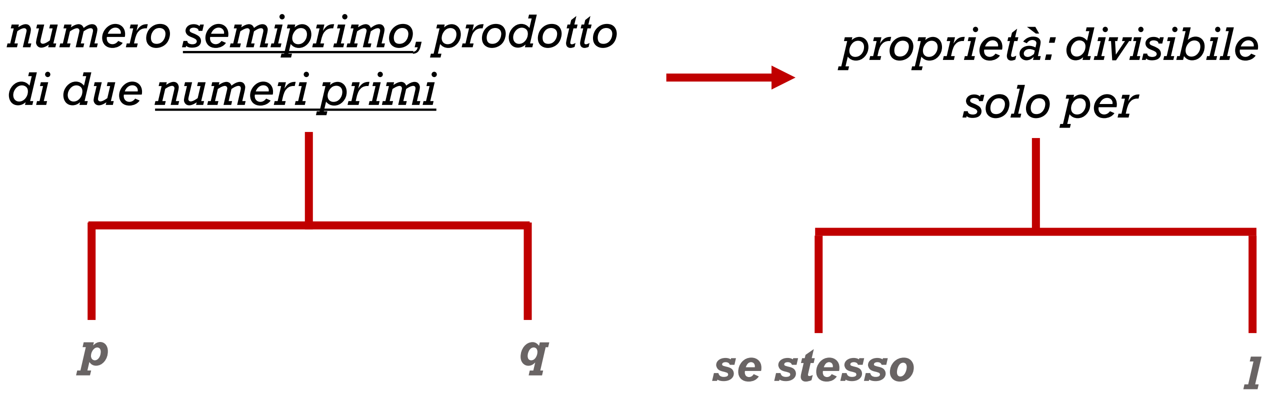
1

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = **55**



numero semiprimo, prodotto di due numeri primi

proprietà: divisibile solo per

p

q

se stesso

1

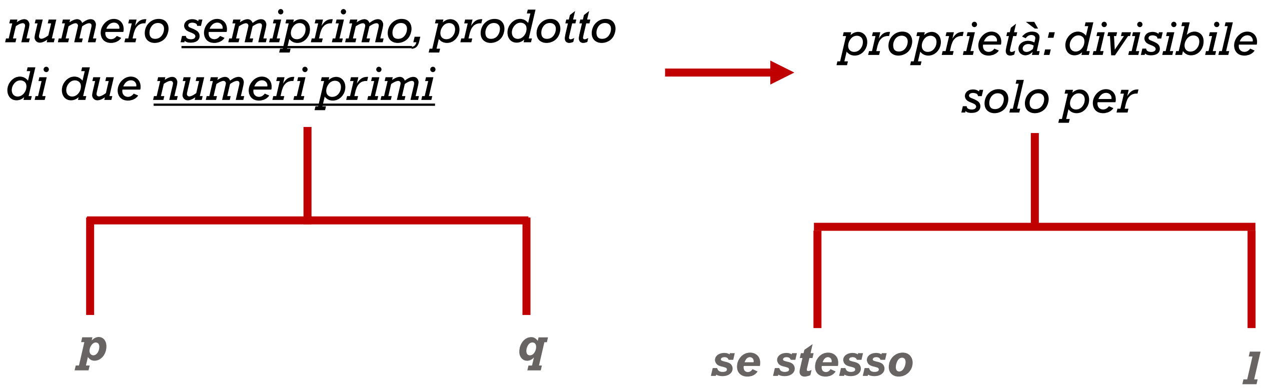
7 (OK)

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55



numero semiprimo, prodotto di due numeri primi → *proprietà: divisibile solo per*

p *q*

se stesso *1*

7 (OK) **99 (NO)**

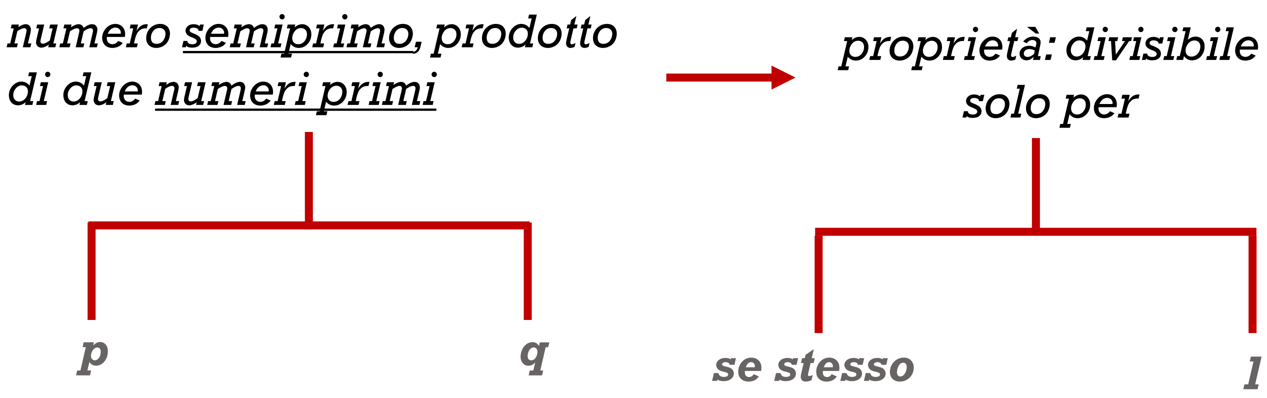
FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = **55**

p = **5**



numero <u>semiprimo</u>, prodotto di due <u>numeri primi</u>

→

proprietà: divisibile solo per

p

q

se stesso

1

5

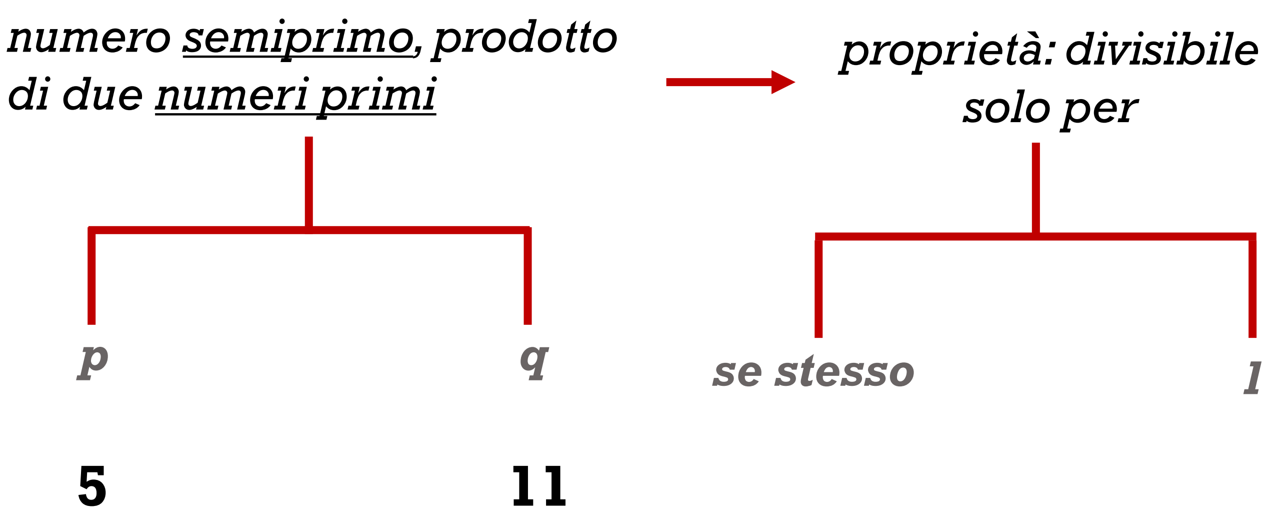
FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55

p = 5 q = 11



numero semiprimo, prodotto di due numeri primi → *proprietà: divisibile solo per*

p — q

5 — 11

se stesso — *1*

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

$n = 55$ $e = 3$

$p = 5$ $q = 11$

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3

p = 5 *q* = 11

- Esponente

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = **55** **e** = **3**

p = **5** q = **11**

- Esponente

- **n** ed **e** devono essere coprimi tra loro

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3

p = 5 *q* = 11

- Esponente

- **n** ed **e** devono essere coprimi tra loro

- **GCD** (Massimo comune divisore) uguale a **1**

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

$n = 55$ $e = 3$ $d = 27$

$p = 5$ $q = 11$

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3 **d** = 27

p = 5 q = 11

inverse_mod(e, (p - 1) * (q - 1))

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3 **d** = 27

p = 5 *q* = 11

inverse_mod(e, (*p* - 1) * (*q* - 1))

3

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3 **d** = 27

p = 5 *q* = 11

inverse_mod(e, (*p* - 1) * (*q* - 1))

3 4

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3 **d** = 27

p = 5 *q* = 11

inverse_mod(e, (*p* - 1) * (*q* - 1))

3 4 * 10

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3 **d** = 27

$p = 5$ $q = 11$

inverse_mod(**e**, (p - 1) * (q - 1))

$$\begin{array}{ccc} 3 & 4 & * \ 10 \\ \hline 3 & & 40 \end{array}$$

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 e = 3 d = 27

***p* = 5 *q* = 11**

inverse_mod(e, (*p* - 1) * (*q* - 1))

3 4 * 10

3 40

modulo inverso di **3** su base **40**

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = **55** **e** = **3** **d** = **27**

p = **5** q = **11**

inverse_mod(e, (p - 1) * (q - 1))

3 * 1 mod 40 = 1 (NO)

$$\frac{3 \quad 4 \quad * \quad 10}{3 \qquad 40}$$

modulo inverso di **3** su base **40**

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3 **d** = 27

p = 5 *q* = 11

inverse_mod(e, (*p* - 1) * (*q* - 1))

3 * 1 mod 40 = 1 (NO)

3 * 2 mod 40 = 1 (NO)

$$\begin{array}{ll} 3 & 4 * 10 \\ \hline 3 & 40 \end{array}$$

modulo inverso di 3 su base 40

Winter 2018 Edition

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = **55** **e** = **3** **d** = **27**

p = **5** *q* = **11**

inverse_mod(**e**, (*p* - 1) * (*q* - 1))

3 * 1 mod 40 = 1 (NO)

3 * 2 mod 40 = 1 (NO)

3 * 3 mod 40 = 1 (NO)

$$\frac{3 \quad 4 \quad * \; 10}{3 \qquad 40}$$

modulo inverso di **3** su base **40**

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 e = 3 d = 27

***p* = 5 *q* = 11**

inverse_mod(e, (*p* - 1) * (*q* - 1))

3 * 1 mod 40 = 1 (NO)
3 * 2 mod 40 = 1 (NO)
3 * 3 mod 40 = 1 (NO)
3 * 4 mod 40 = 1 (NO)

3 4 * 10

3 40

modulo inverso di **3** su base **40**

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = **55** **e** = **3** **d** = **27**

p = **5** q = **11**

inverse_mod(e, (p - 1) * (q - 1))

3 * 1 mod 40 = 1 (NO)
3 * 2 mod 40 = 1 (NO)
3 * 3 mod 40 = 1 (NO)
3 * 4 mod 40 = 1 (NO)
3 * 5 mod 40 = 1 (NO)

3 4 * 10

3 40

modulo inverso di **3** su base **40**

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = **55** **e** = **3** **d** = **27**

p = **5** q = **11**

inverse_mod(e, (p - 1) * (q - 1))

$$\frac{3 \quad 4 \quad * \; 10}{3 \qquad 40}$$

modulo inverso di **3** su base **40**

3 * 1 mod 40 = 1 (NO)
3 * 2 mod 40 = 1 (NO)
3 * 3 mod 40 = 1 (NO)
3 * 4 mod 40 = 1 (NO)
3 * 5 mod 40 = 1 (NO)
[...]

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = **55** **e** = **3** **d** = **27**

p = **5** *q* = **11**

3 * 1 mod 40 = 1 (NO)
3 * 2 mod 40 = 1 (NO)
3 * 3 mod 40 = 1 (NO)
3 * 4 mod 40 = 1 (NO)
3 * 5 mod 40 = 1 (NO)
[...]
3 * 27 mod 40 = 1 (**SI!**)

inverse_mod(e, (*p* - 1) * (*q* - 1))

3 4 * 10

3 40

modulo inverso di **3** su base **40**

HACK IN BO® Winter 2018 Edition

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = **55** **e** = **3** **d** = $\boxed{27}$

p = **5** ***q*** = **11**

3 * 1 mod 40 = 1 (NO)

3 * 2 mod 40 = 1 (NO)

3 * 3 mod 40 = 1 (NO)

3 * 4 mod 40 = 1 (NO)

3 * 5 mod 40 = 1 (NO)

[...]

3 * $\boxed{27}$ mod 40 = 1 (**SI!**)

inverse_mod(e, (*p* - 1) * (*q* - 1))

$$\frac{\mathbf{3} \quad \mathbf{4} \quad \mathbf{*} \ \mathbf{10}}{\mathbf{3} \qquad \mathbf{40}}$$

modulo inverso di **3** su base **40**

HackInBo Winter 2018 Edition

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3 **d** = 27

$p = 5 \quad q = 11$

inverse_mod(e, $(p - 1) * (q - 1)$)

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 e = 3 d = 27

p = 5 q = 11

inverse_mod($\boxed{e}$, (p - 1) * (q - 1))

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3 **d** = 27

p = 5 q = 11

$$\mathrm{inverse\_mod}(\boxed{e}, (\boxed{p} - 1) * (\boxed{q} - 1))$$

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3 **d** = 27

$p = 5$ $q = 11$

$$\text{inverse\_mod}(\boxed{e}, (\boxed{p} - 1) * (\boxed{q} - 1))$$

sicurezza RSA ruota attorno a **p** e **q**

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

$n = 55$ $e = 3$ $d = 27$

$p = 5$ $q = 11$

$$\text{inverse\_mod}(\boxed{e}, (\boxed{p} - 1) * (\boxed{q} - 1))$$

sicurezza RSA ruota attorno a **p** e **q**

HackInBo Winter 2018 Edition

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

n = 55 **e** = 3 **d** = 27

p = 5 *q* = 11

inverse_mod(e, (*p* - 1) * (*q* - 1))

sicurezza RSA ruota attorno a **p** e **q**

…la verità è che è anche peggio di così!

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

inverse_mod(e, (*p* - 1) * (*q* - 1))

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

inverse_mod(e, (p - 1) * (q - 1))

n = 55

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

inverse_mod(e, (p - 1) * (q - 1))

n = 55 ... p = 5

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

inverse_mod(e, (*p* - 1) * (*q* - 1))

n = 55 … *p* = 5

q* = n / *p

FATTORIZZAZIONE CHIAVE RSA

inverse_mod(e, (p - 1) * (q - 1))

n = 55 … p = 5

q = n / p

q = 11

FATTORIZZAZIONE CHIAVE RSA

CRICCO

IT (SON)

inverse_mod(e, (p - 1) * (q - 1))

n = 55 … q = 11

p = n / q

p = 5

FATTORIZZAZIONE CHIAVE RSA

inverse_mod(e, (p - 1) * (q - 1))

n = 55 … q = 11

p = n / q

p = 5

…non bisogna fattorizzare due numeri. Basta scoprirne uno solo per rompere RSA!!!

CRICCO

IT (SON)

p =

1539968640381254945832235930739012986038972099588258698710371172852272279442296686218866199458552739613291021869286401781690890685476902925787727881900866122499077663766536275099968282649215660609816179975946174964738586546867130304099752130399387289403794106006892831093471700262984193137566918937884611405095

q =

1480335472004634163213209681368440605491144208431091039251938370312610979885152342240087152980357320071849952380958356109410664297319399246756474668001343151808450565226466318587282756964218440129313914124761801098622909839092915416569347530813254345868999246504606657825786765940637462115290522641510072286795

ENTER SIDE CHANNEL…

CRICCO

IT (SON)

p =
1539968640381254945832235930739012986038972099588258698710371172852272279442296686218866199458552739613291021869286401781690890685476902925787727881900866122499077663766536275099968282649215660609816179975946174964738586546867130304099752130399387289403794106006892831093471700262984193137566918937884611405 09

q =
1480335472004634163213209681368440605491144208431091039251938370312610979885152342240087152980357320071849952380958356109410664297319399246756474668001343151808450565226466318587282756964218440129313914124761801098622909839092915416569347530813254345868999246504606657825786765940637462115290522641510072 28679

M^{65537}

RSA

ENCRYPTION -> $C \equiv m^e \bmod n$

VERIFICA -> $V \equiv c^e \bmod n$

RSA

DECRYPTION -> $\mathbf{M} = c^{d} \ mod\ n$

FIRMA -> $\mathbf{S} = m^{d} \ mod\ n$

101003682984200292473213491110009319058651343981
87644848851277991154261760129168069853535169143
912167910298840266211781105627700072842578484865
309715590051367279842732179028698684455218792798
058076230379388932302217539101718112733573141780
839073344575675376128646369098114519747438177585
C555811413897

RSA-CRT: OTTIMIZZAZIONE

RSA-CRT: OTTIMIZZAZIONE

- Valori precalcolati:
  - **qInv** = (1/q) mod p
  - **dP** = d (mod p - 1)
  - **dQ** = d (mod q - 1)

RSA-CRT: OTTIMIZZAZIONE

- Valori precalcolati:
  - **qInv** = (1/q) mod p
  - **dP** = d (mod p - 1)
  - **dQ** = d (mod q - 1)

- Calcolati dinamicamente:
  - **s1** = m^dP mod p
  - **s2** = m^dQ mod q
  - **h** = (s1 - s2) * qInv mod p
  - **m** = s2 + q * h

RSA-CRT: OTTIMIZZAZIONE

- Valori precalcolati:
  - **qInv** = (1/q) mod p
  - **dP** = d (mod p - 1)
  - **dQ** = d (mod q - 1)

- Calcolati dinamicamente:
  - **s1** = m^dP mod p
  - **s2** = m^dQ mod q
  - **h** = (s1 - s2) * qInv mod p
  - **m** = s2 + q * h

Se durante il calcolo di s1 o s2 avviene un errore lato server (i.e. hardware fault), una firma digitale RSA "difettosa" viene calcolata ed un fattore primo di RSA può essere recuperate con la formula:

$$\mathrm{gcd}(Y^e - x, n)$$

RSA-CRT: OTTIMIZZAZIONE

- Valori precalcolati:
  - **qInv** = (1/q) mod p
  - **dP** = d (mod p - 1)
  - **dQ** = d (mod q - 1)

- Calcolati dinamicamente:
  - **s1** = m^dP mod p
  - **s2** = m^dQ mod q
  - **h** = (s1 - s2) * qInv mod p
  - **m** = s2 + q * h

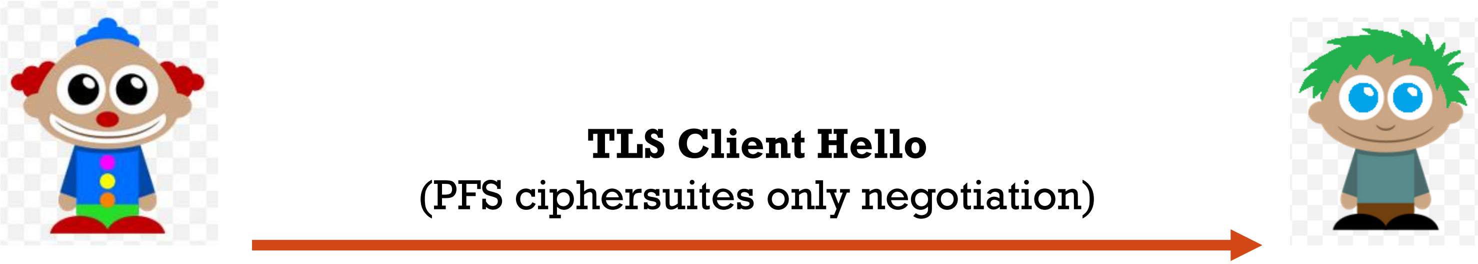
Se durante il calcolo di s1 o s2 avviene un errore lato server (i.e. hardware fault), una firma digitale RSA "difettosa" viene calcolata ed un fattore primo di RSA può essere recuperate con la formula:

$$\boxed{\gcd(Y^e - x,\ n)}$$

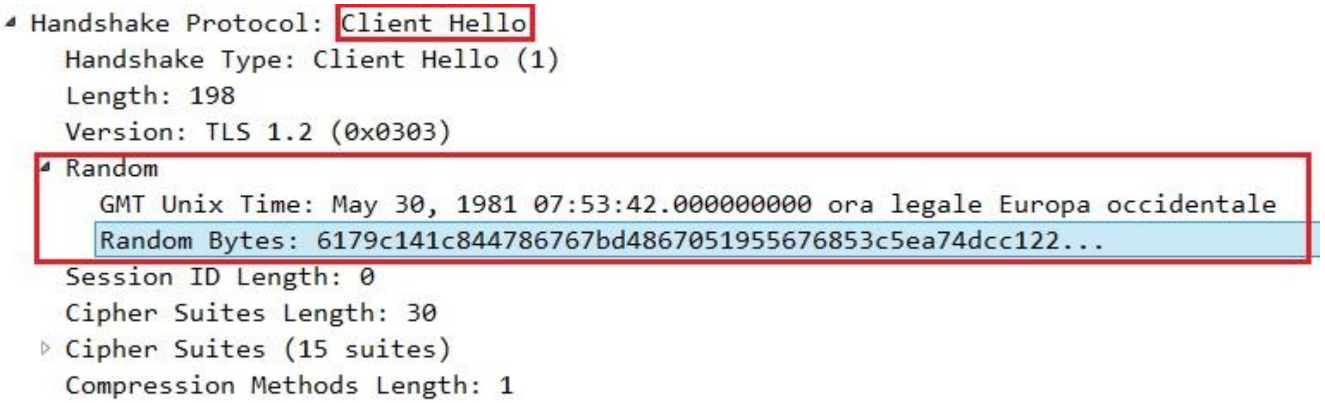
Lenstra Attack 1996

SSL/TLS

SSL/TLS

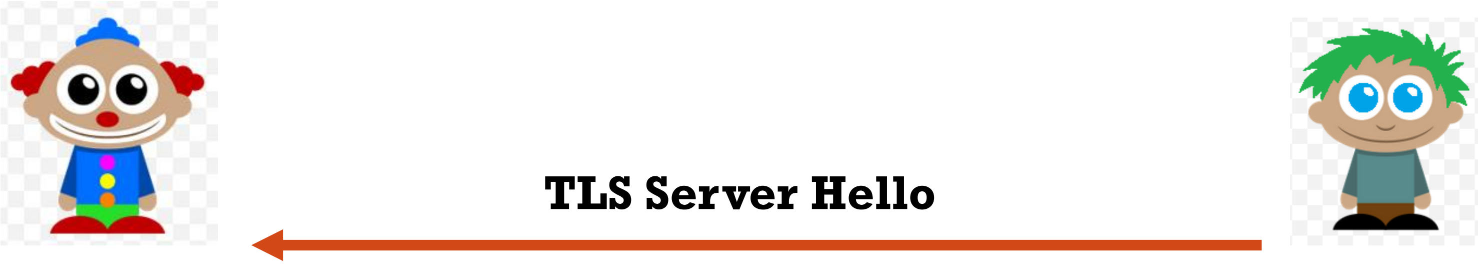


TLS Client Hello
(PFS ciphersuites only negotiation)

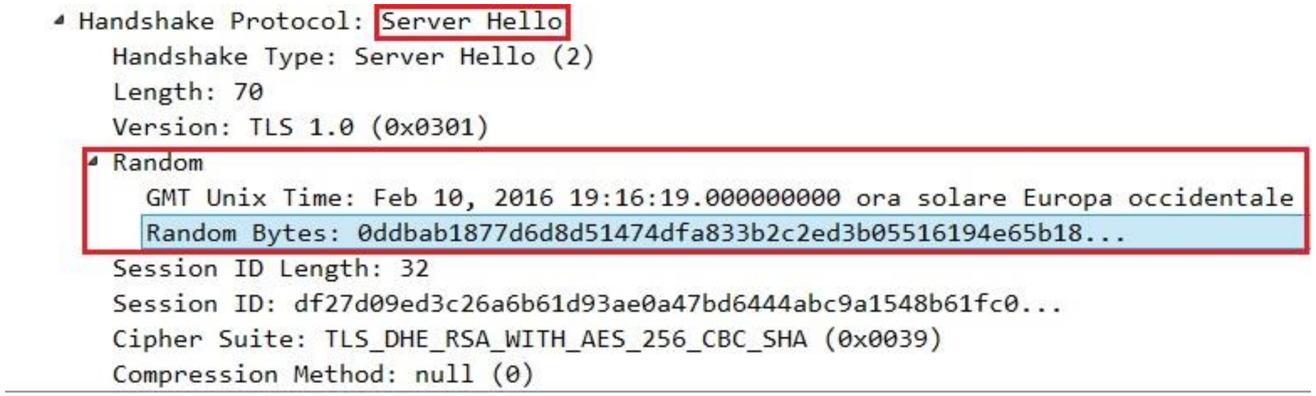


```
◢ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 198
    Version: TLS 1.2 (0x0303)
  ◢ Random
      GMT Unix Time: May 30, 1981 07:53:42.000000000 ora legale Europa occidentale
      Random Bytes: 6179c141c844786767bd4867051955676853c5ea74dcc122...
    Session ID Length: 0
    Cipher Suites Length: 30
  ▷ Cipher Suites (15 suites)
    Compression Methods Length: 1
```

SSL/TLS



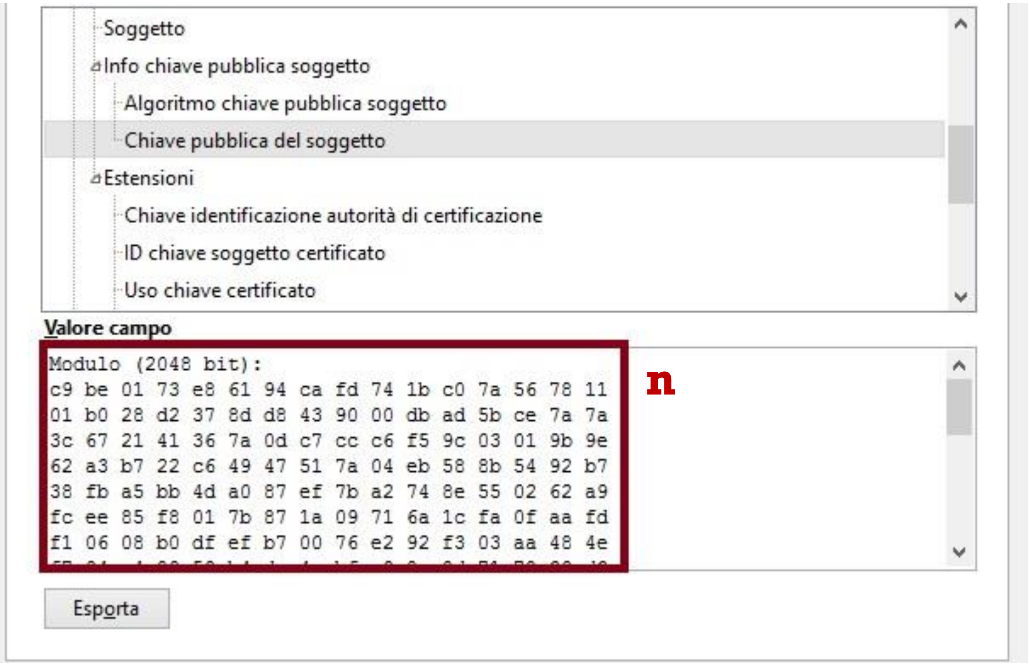
TLS Server Hello



```
◢ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 70
    Version: TLS 1.0 (0x0301)
  ◢ Random
      GMT Unix Time: Feb 10, 2016 19:16:19.000000000 ora solare Europa occidentale
      Random Bytes: 0ddbab1877d6d8d51474dfa833b2c2ed3b05516194e65b18...
    Session ID Length: 32
    Session ID: df27d09ed3c26a6b61d93ae0a47bd6444abc9a1548b61fc0...
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
    Compression Method: null (0)
```

SSL/TLS

TLS Server Certificate



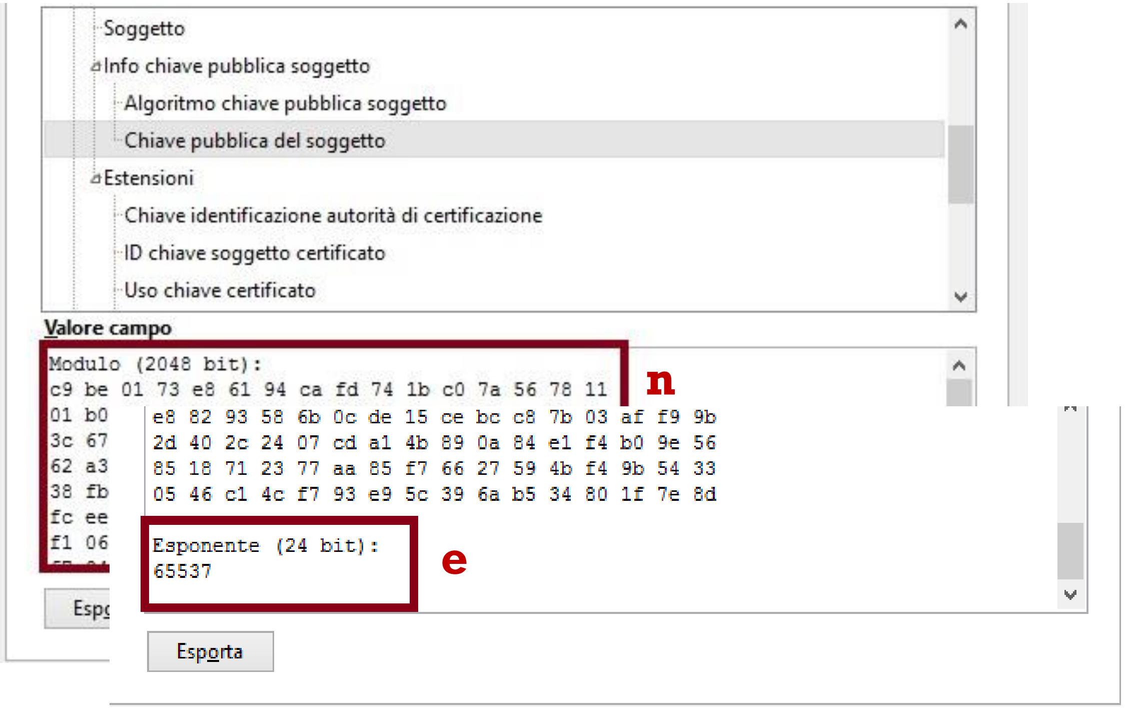
Soggetto
Info chiave pubblica soggetto
Algoritmo chiave pubblica soggetto
Chiave pubblica del soggetto
Estensioni
Chiave identificazione autorità di certificazione
ID chiave soggetto certificato
Uso chiave certificato
Valore campo
Esporta

```
Modulo (2048 bit):
c9 be 01 73 e8 61 94 ca fd 74 1b c0 7a 56 78 11
01 b0 28 d2 37 8d d8 43 90 00 db ad 5b ce 7a 7a
3c 67 21 41 36 7a 0d c7 cc c6 f5 9c 03 01 9b 9e
62 a3 b7 22 c6 49 47 51 7a 04 eb 58 8b 54 92 b7
38 fb a5 bb 4d a0 87 ef 7b a2 74 8e 55 02 62 a9
fc ee 85 f8 01 7b 87 1a 09 71 6a 1c fa 0f aa fd
f1 06 08 b0 df ef b7 00 76 e2 92 f3 03 aa 48 4e
```

n

SSL/TLS

TLS Server Certificate



- Soggetto
- Info chiave pubblica soggetto
  - Algoritmo chiave pubblica soggetto
  - Chiave pubblica del soggetto
- Estensioni
  - Chiave identificazione autorità di certificazione
  - ID chiave soggetto certificato
  - Uso chiave certificato

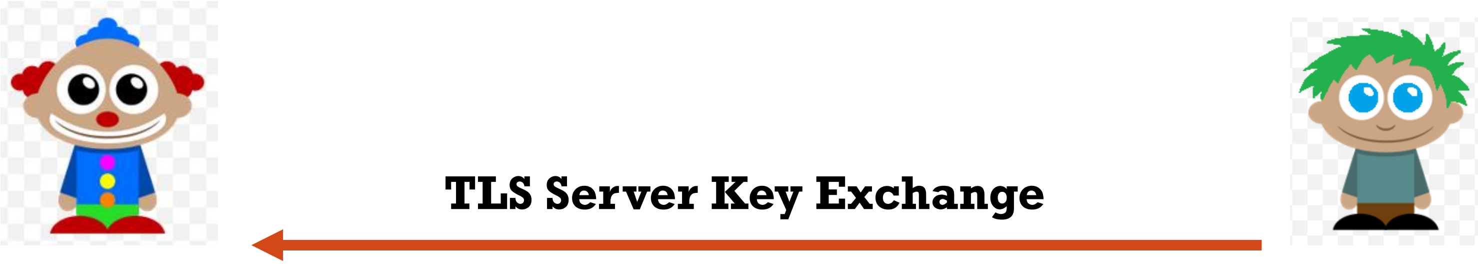
Valore campo

```
Modulo (2048 bit):
c9 be 01 73 e8 61 94 ca fd 74 1b c0 7a 56 78 11
01 b0    e8 82 93 58 6b 0c de 15 ce bc c8 7b 03 af f9 9b
3c 67    2d 40 2c 24 07 cd a1 4b 89 0a 84 e1 f4 b0 9e 56
62 a3    85 18 71 23 77 aa 85 f7 66 27 59 4b f4 9b 54 33
38 fb    05 46 c1 4c f7 93 e9 5c 39 6a b5 34 80 1f 7e 8d
fc ee
f1 06    Esponente (24 bit):
         65537
```

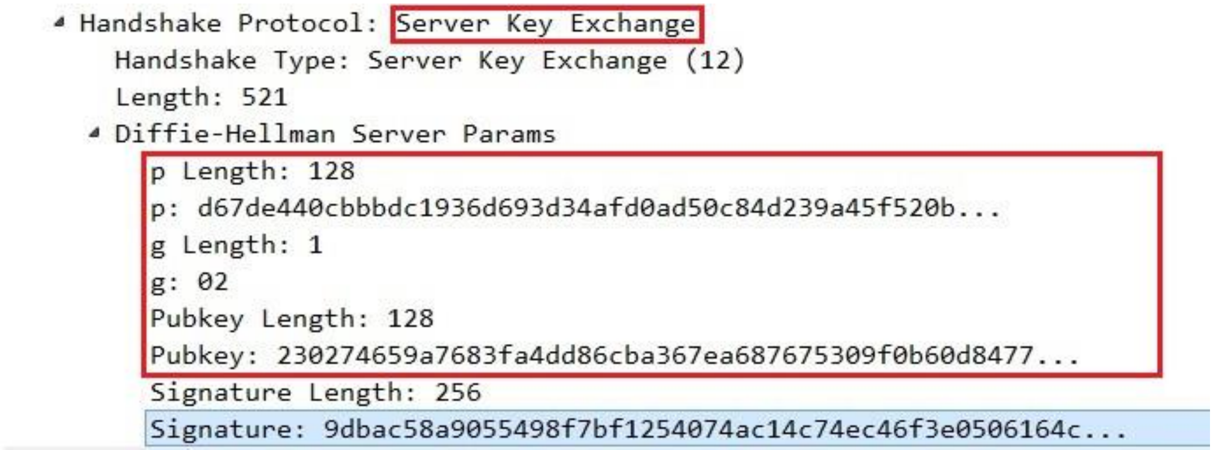
n

e

SSL/TLS



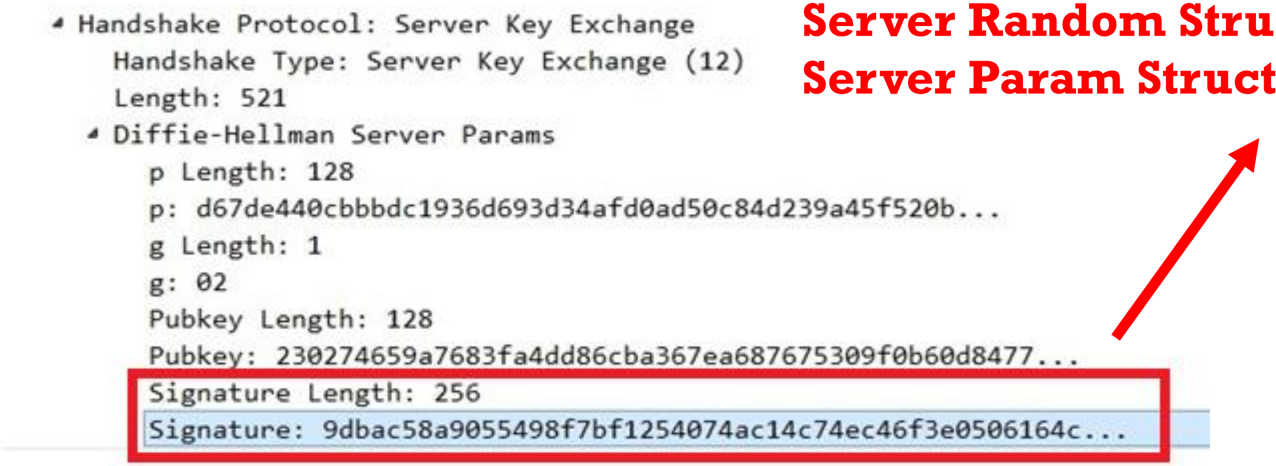
TLS Server Key Exchange



```
◢ Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 521
  ◢ Diffie-Hellman Server Params
      p Length: 128
      p: d67de440cbbbdc1936d693d34afd0ad50c84d239a45f520b...
      g Length: 1
      g: 02
      Pubkey Length: 128
      Pubkey: 230274659a7683fa4dd86cba367ea687675309f0b60d8477...
      Signature Length: 256
      Signature: 9dbac58a9055498f7bf1254074ac14c74ec46f3e0506164c...
```

SSL/TLS

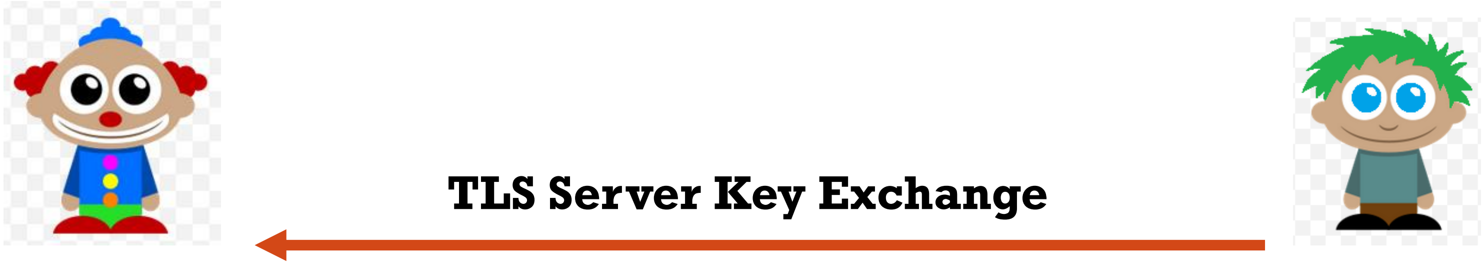
TLS Server Key Exchange



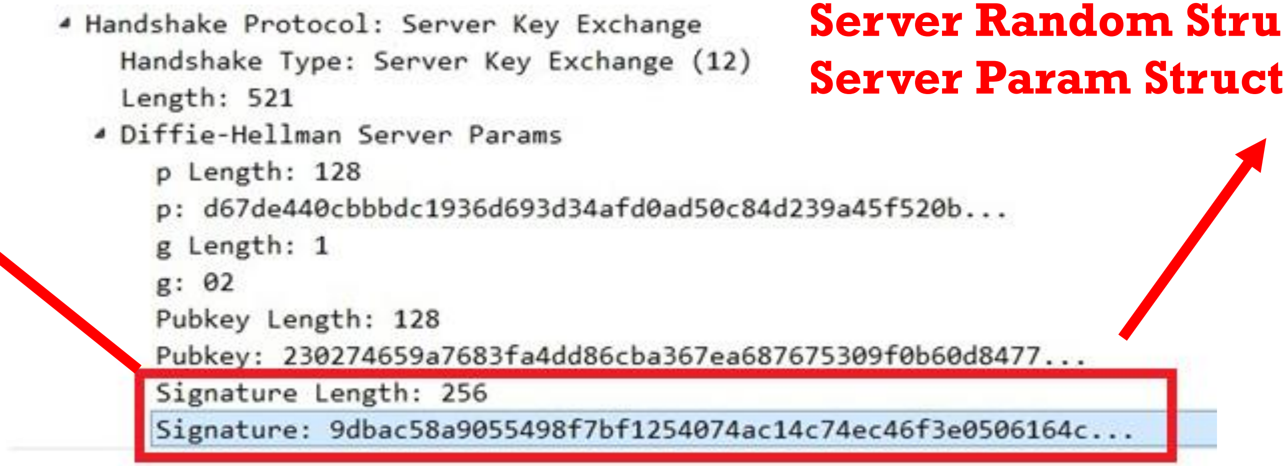
```
◢ Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 521
  ◢ Diffie-Hellman Server Params
      p Length: 128
      p: d67de440cbbbdc1936d693d34afd0ad50c84d239a45f520b...
      g Length: 1
      g: 02
      Pubkey Length: 128
      Pubkey: 230274659a7683fa4dd86cba367ea687675309f0b60d8477...
      Signature Length: 256
      Signature: 9dbac58a9055498f7bf1254074ac14c74ec46f3e0506164c...
```

Client Random Struct (*Client Hello Message*)
Server Random Struct (*Server Hello Message*)
Server Param Struct (*Key Exchange Message*)

SSL/TLS



Se la firma digitale calcolata dal server è invalida, l’attaccante applica Lenstra attack e genera chiave privata del server (anche in passive mode!)



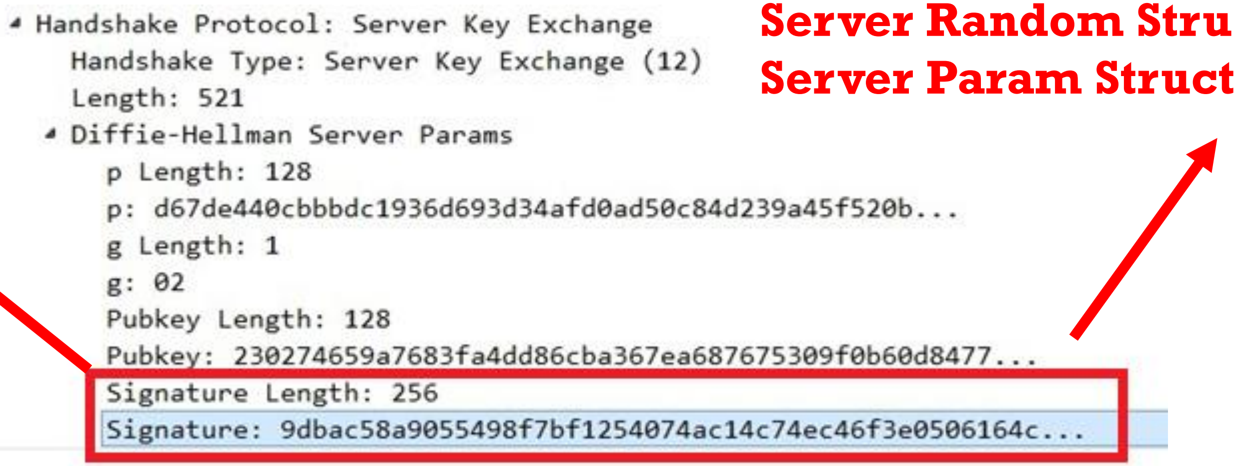
```
◢ Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 521
  ◢ Diffie-Hellman Server Params
      p Length: 128
      p: d67de440cbbbdc1936d693d34afd0ad50c84d239a45f520b...
      g Length: 1
      g: 02
      Pubkey Length: 128
      Pubkey: 230274659a7683fa4dd86cba367ea687675309f0b60d8477...
      Signature Length: 256
      Signature: 9dbac58a9055498f7bf1254074ac14c74ec46f3e0506164c...
```

Client Random Struct (*Client Hello Message*)
Server Random Struct (*Server Hello Message*)
Server Param Struct (*Key Exchange Message*)

SSL/TLS

TLS Server Key Exchange

Se la firma digitale calcolata dal server è invalida, l’attaccante applica Lenstra attack e genera chiave privata del server (anche in passive mode!)



```
◢ Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 521
  ◢ Diffie-Hellman Server Params
      p Length: 128
      p: d67de440cbbbdc1936d693d34afd0ad50c84d239a45f520b...
      g Length: 1
      g: 02
      Pubkey Length: 128
      Pubkey: 230274659a7683fa4dd86cba367ea687675309f0b60d8477...
      Signature Length: 256
      Signature: 9dbac58a9055498f7bf1254074ac14c74ec46f3e0506164c...
```

Client Random Struct (*Client Hello Message*)
Server Random Struct (*Server Hello Message*)
Server Param Struct (*Key Exchange Message*)

Lenstra Attack 1996

$\gcd(Y^{e} - x, n)$

DEMO

SLIDE: HTTPS://WWW.BLACKHAT.COM/DOCS/US-16/MATERIALS/US-16-ORTISI-RECOVER-A-RSA-PRIVATE-KEY-FROM-A-TLS-SESSION-WITH-PERFECT-FORWARD-SECRECY.PDF

WHITEPAPER: HTTP://WWW.SEGFAULT.IT/TOOLS/BLACKHAT2016US-WP.PDF

TOOL SOURCE CODE: HTTP://WWW.SEGFAULT.IT/TOOLS/TOOLS-LATEST.ZIP

THE END

CONOSCERE LA CRITTOGRAFIA ROMPENDOLA

HackInBo®
Winter 2018 Edition