BLUENET

There is always more than one solution

Società incubata e accelerata da

Campania NewSteel

CHI SIAMO

BLUENET

Bluenet srl, start up innovativa nel settore dell'ICT, nata nel 2014, sviluppa nuovi programmi di ricerca, sviluppo e applicazione di carattere scientifico e tecnologico nei campi **dell'informatica, telecomunicazioni ed elettronica**. L'azienda, che ha una consolidata esperienza nel settore delle smartcard, dei microchip e dei sistemi operativi per microcontrollori e NFC (Near Field Communication), possiede **due brevetti** ed ha sviluppato delle tecnologie mature che puntano a superare i prodotti tradizionali dei relativi mercati di rifermento.

ESPERIENZA

BLUENET

- *SVILUPPO SOFTWARE*

  C/C++, #NET, Java, Servlet, Apache-Tomcat, MySql, ARM-Cortex , Object-c/swift

- *SVILUPPO FIRMWARE*

  ISO 7816, ISO 14443, ISO 15693, ISO 10373, ISO 18013, EMV Standard, JAVA Card technology

- *CRITTOGRAFIA*

  Symmetric Key, Algorithm: DES(FIPS46-3), TDES, AES, Diffie Hellman, RSA, EAC, ECC, ISO 9796, ISO 9797, ISO 10116, ISO 10118, FIPS140-2

- *BIOMETRIA*

  FVC2004, PFT II, *POEBVA,* AFIS, SHA256

CRITTOGRAFIA

BLUENET

SISTEMI CRITTOGRAFICI SONO USATI UN PO' OVUNQUE ED IN QUALSIASI PERIODO STORICO

MESSAGGIO IN CHIARO:

LA CRITTOGRAFIA E' L'ARTE DI RENDERE SEGRETI I MESSAGGI

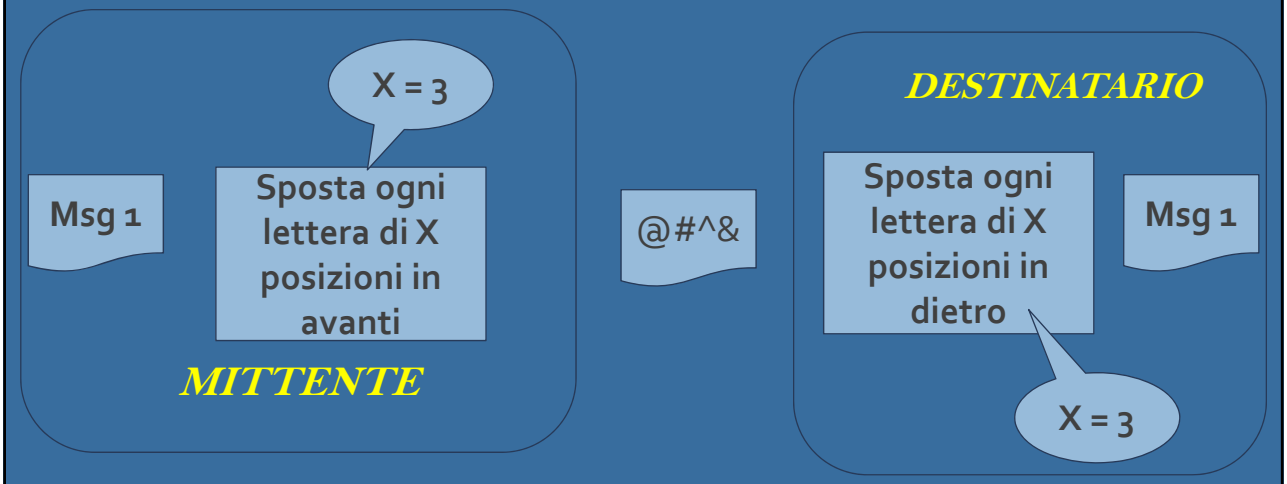
MESSAGGIO CIFRATO:

OD FUNZZRLUDIND H' O'DUZH GN UHQGHUH VHLUHZN N PHVVDLLN

SOLO CHI CONOSCE LA REGOLA "SPOSTA DI TRE" PUÒ DECIFRARE IL MESSAGGIO

CRITTOGRAFIA

LA CRITTOGRAFIA SI COMPONE DI DUE ELEMENTI ESSENZIALI:
ALGORITMO E CHIAVE



CRITTOGRAFIA

Fissato l'algoritmo di cifratura l'unica possibilità di decifrare il messaggio è provare, una per volta, tutte le possibili chiavi fino a trovare quella giusta.

LA SICUREZZA DI UN SISTEMA CRITTOGRAFICO È LEGATA ALLA CHIAVE

LUNGHEZZA DELLA CHIAVE:

BIT: UNITÀ DI MISURA DELL'INFORMAZIONE (BINARY DIGIT)

$20 = (10100)_2$ $2^1=2$ $2^2=4$ ….. $2^5=32$

….. $2^{56}=72057594037927936$

20 : 2 = 10 RESTO 0
10 : 2 = 5 RESTO 0
5 : 2 = 2 RESTO 1
2 : 2 = 1 RESTO 0
1 : 2 = 0 RESTO 1

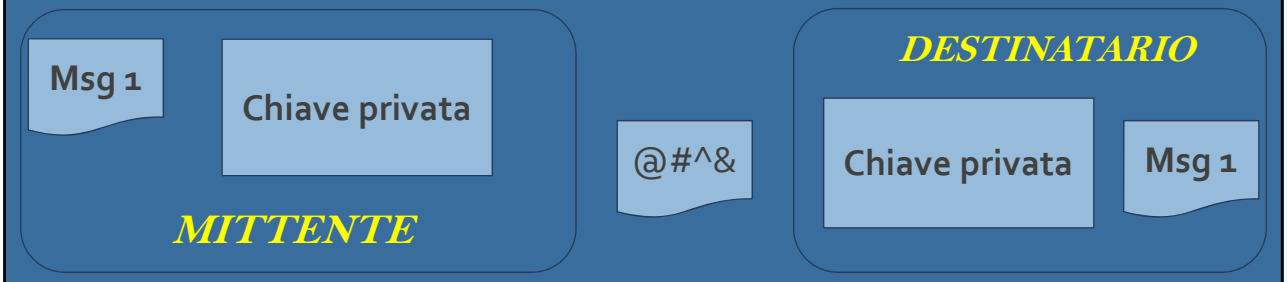
I POSSIBILI VALORI DELLA CHIAVE CRESCONO ESPONENZIALMENTE CON LA LUNGHEZZA DELLA STESSA

CRITTOGRAFIA

BLUENET

ALGORITMI A CHIAVE PRIVATA O SIMMETRICI

DES – CHIAVE 56 BIT, TDES CHIAVE 168



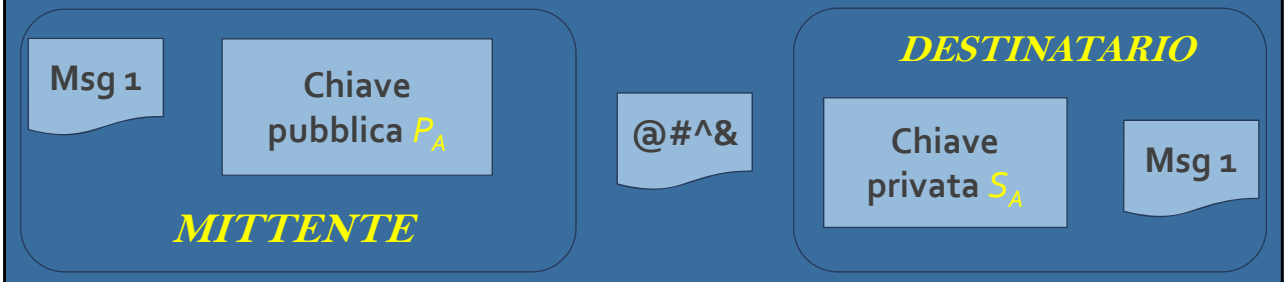
Hanno il vantaggio di essere veloci, idonei per cifrare grandi moli di dati ma richiedono la DISTRIBUZIONE DELLA CHIAVE PRIVATA A TUTTI I DESTINATARI

CRITTOGRAFIA

BLUENET

ALGORITMI A CHIAVE PUBBLICA O ASIMMETRICI

RSA, ECC



LA CHIAVE PUBBLICA PUÒ ESSERE DISTRIBUITA,

SOLO LA CHIAVE PRIVATA DEVE ESSERE TENUTA NECESSARIAMENTE SEGRETA

CRITTOGRAFIA

RSA SI BASA SULLA MOLTIPLICAZIONE DI DUE NUMERI PRIMI p, q

- CALCOLARE $n = p \times q$ È FACILE
- CALCOLARE p, q DA n È DIFFICILE A MENO CHE NON SI CONOSCA UNO DEI DUE

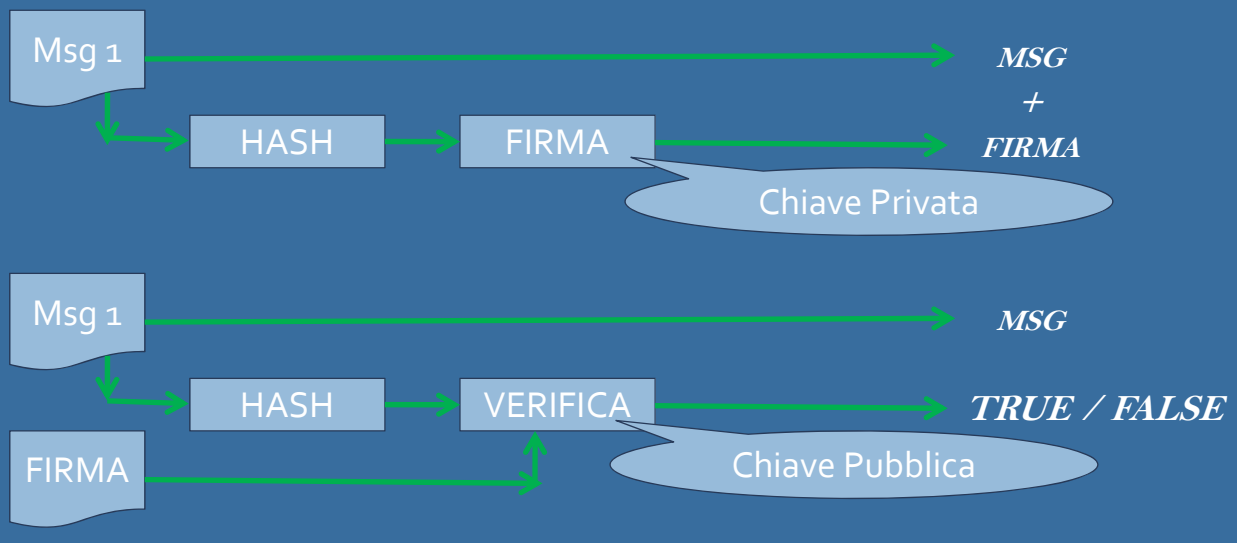
MITTENTE: SCEGLIE I DUE NUMERI PRIMI per esempio $p = 5$, $q = 11$;
CALCOLA $p \times q = 55$, $(p-1) \times (q-1) = 40$;
SCEGLIE $e<40$ per esempio $e=7$;
CALCOLA d TALE CHE $e \times d$ MOD $40 = 1$ ($d=23$ infatti $7 \times 23 = 160+1$);
PUBBLICA LA CHIAVE PUBBLICA: $P_A = (e, n) = (7,55)$;
TIENE SEGRETA LA CHIAVE PRIVATA: $S_A = d = 23$.

DESTINATARIO: PER SPEDIRE IL MESSAGGIO $M<55$ CALCOLA $C=M^e$ MOD $n = M^7$ MOD 55

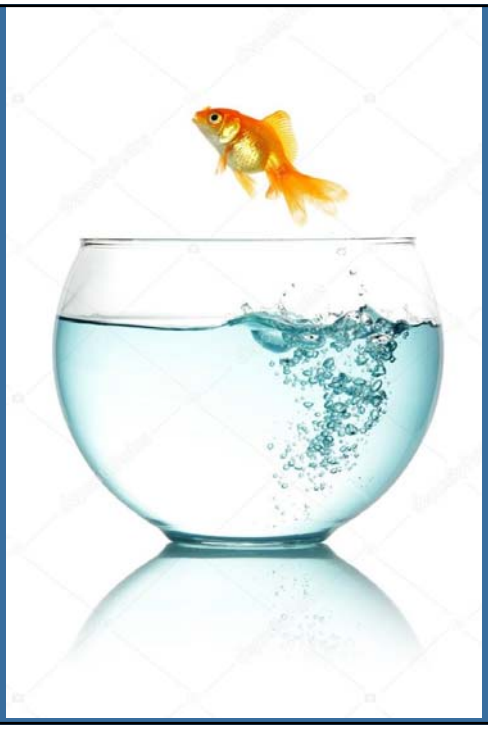
MITTENTE: PER DECODIFICARE IL MESSAGGIO CALCOLA $M = C^d$ MOD $n = C^{23}$ MOD 55

CRITTOGRAFIA

LA FIRMA DIGITALE



BLUENET



ESPERIENZA

BLUENET

TRASPORTI (TPL)

TRENITALIA
GRUPPO FERROVIE DELLO STATO

atac ROMA

GTT GRUPPO TORINESE TRASPORTI

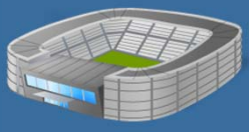
ataf

T per

EAVsrl Ente Autonomo Volturno

ARCEA

CONTROL ACCESS SYSTEM



a2a

Lalilauro

JUVENTUS

N

e-ID TECHNOLOGY

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

ENGINEERING

TIM

LA SQUADRA

BLUENET

BREVETTI

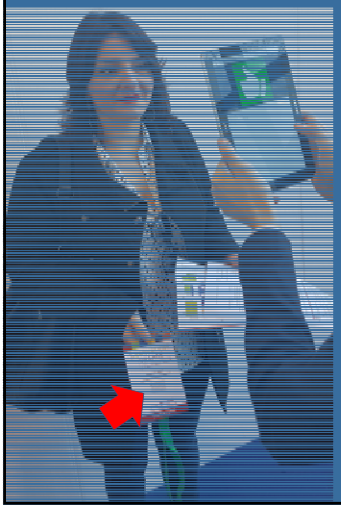
BLUENET

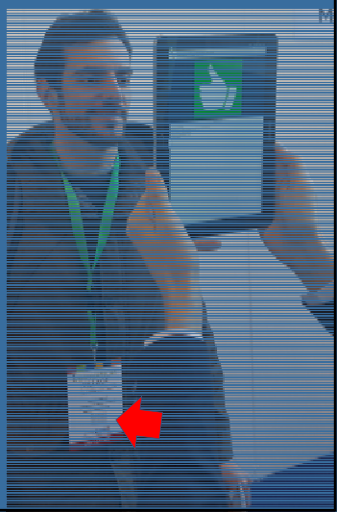
OSCAR – Over the Smart CARd

BREVETTI

BLUeCODE – la sicurezza di un chip stampata su carta

BLUeCODE
MULTIPLE SECURITY LEVELS





BLUeCODE
MULTIPLE SECURITY LEVELS

Se utilizzassimo il BLUeCODE questo biglietto avrebbe i dati del Sig. XXXgenio e chiunque sarebbe scoraggiato ad acquistarlo, perché sarebbe impossibile accedere all'evento a chiunque tranne che al proprietario.

«E se non posso andarci più?»
C'è sempre il «cambio nome» ma allo stesso prezzo d'acquisto e sulla stessa piattaforma di rivendita ticket.

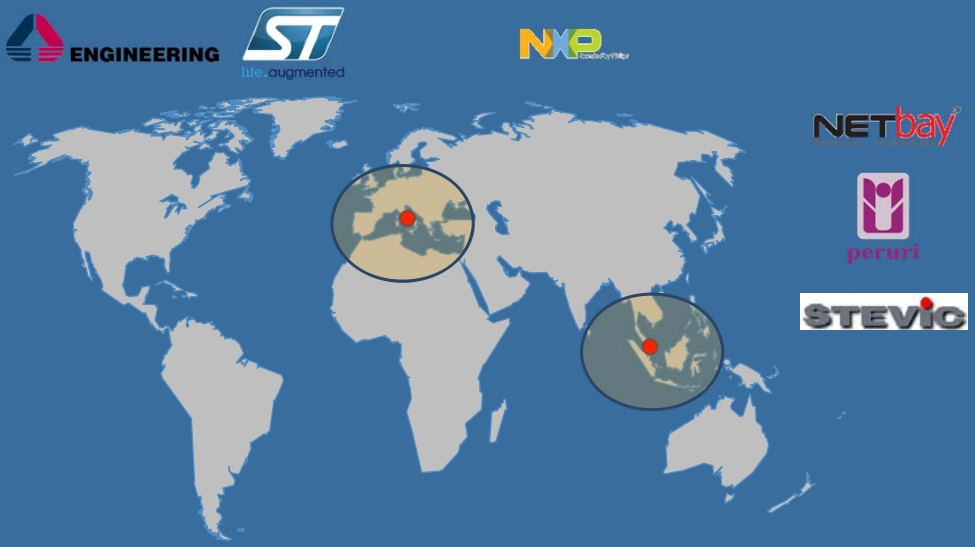
IoTOURIST

IoTourist è programmabile in base alle preferenze del turista ed alle convenzioni attivate, presso i centri autorizzati. Il turista sceglierà o essere guidato dagli operatori locali.

- Il turista giunge nel comune interessato
- I punti di accoglienza e gli esercenti abilitati accolgono le richieste del turista
- Il turista, guidato, sceglie i percorsi e le strutture da visitare, i mezzi di trasporto necessari per raggiungere le destinazioni, eventuali sconti e promozioni da inserire nel «Pacchetto IoTourist» e infine quanto credito caricare sul dispositivo
- Il punto di accoglienza programma opportunamente IoTourist ed effettua la vendita



GLOBAL PARTNERS



Italia
Città della Scienza
Via Coroglio, 57,
80124, Napoli (NA)

Singapore
37 Senang Crescent,
416606, Singapore
(SG)

Grazie per l'attenzione

Nicola Fedele
Email: info@bluenet.com.sg

BLUENET

PARLANO DI NOI