LICEO STATALE "ENRICO MEDI"

CON INDIRIZZI: *SCIENTIFICO – SCIENTIFICO SCIENZE APPLICATE - LINGUISTICO – SCIENZE UMANE – ECONOMICO SOCIALE - CLASSICO*

Sede: VIA MAGENTA, 7/A - 37069 VILLAFRANCA di VERONA - Tel. 045.7902067 Fax : 045.6300817

e-mail sede: info@liceomedi.com - Preside : preside@liceomedi.com

Sito http://www.liceomedi.com

C.F. 80014060232 Codice meccanografico VRPS06000L

Piano Lauree Scientifiche 2013-2014

Verbale del primo incontro con gli studenti: Martedì 12 Novembre 2013, ore 13:45-16:45

Dopo una breve introduzione alle finalità del Progetto "Piano Lauree Scientifiche 2013-2014" dal titolo "Crittografia e crittanalisi", viene illustrato con delle slides lo scopo delle attività che seguiranno, in particolare l'obiettivo finale è far apprezzare ai ragazzi l'utilizzo della matematica nell'ambito della cifratura di messaggi, oggi più che mai necessaria per accessi con credenziali, transazioni bancarie, pagamenti via Internet, ecc.

Viene dapprima dato ai ragazzi un messaggio cifrato (con cifratura di Cesare) che devono decriptare. La cosa non richiede molto tempo, in quanto le parole sono separate dagli spazi. Dopo una breve discussione sui cifrari monoalfabetici, viene dato da decriptare un altro messaggio, questa volta generato utilizzando un cifrario monoalfabetico random. In questo caso, per risalire alla corrispondenza tra lettere in chiaro e lettere cifrate è necessario utilizzare l'analisi statistica delle frequenze.

Infine, viene introtto il disco di Leon Battista Alberti come esempio di cifrario polialfabetico e viene dato da costruire a casa il disco con una sequenza predeterminata delle lettere interne.

Villafranca di Verona, 12 Novembre 2013.

Marco Caliari _____

Simone Zuccher _____

Sede: VIA MAGENTA, 7/A - 37069 VILLAFRANCA di VERONA - Tel. 045.7902067 Fax : 045.6300817
e-mail sede: info@liceomedi.com - Preside : preside@liceomedi.com
Sito http://www.liceomedi.com
C.F. 80014060232 Codice meccanografico VRPS06000L

Piano Lauree Scientifiche 2013-2014

Verbale del secondo incontro con gli studenti: Mercoledì 20 Dicembre 2013, ore 13:45-16:45

Gli studenti vengono divisi in due gruppi ognuno dei quali cripta un messaggio di al massimo dieci parole usando il disco di Leon Battista Alberti precedentemente costruito (inserendo i numeri da 1 a 4 tra le parole e a spezzare le doppie, e sostituendo eventuali H con X e U,V,W con V). Il messaggio criptato viene consegnato all'altro gruppo che dovrà tentare di decriptarlo senza conoscere la chiave. In questo modo si capisce che il metodo di cifratura, pur non essendo attaccabile con l'analisi delle frequenze, non è così difficile da violare. Ogni gruppo decide una chiave (lettera del disco esterno) e riporta come prima lettera del messaggio la lettera interna corrispondente alla chiave. I messaggi vengono scambiati e decrittati dal gruppo opposto.

Cifratura di Vigenere. Spiegazione e crittanalisi (statistiche sui linguaggi naturali). Una chiave lunga e casuale resiste alle analisi statistiche. Cenni di cifratura GSM. Cifrario di Vernam. Problema della distribuzione delle chiavi.

Villafranca di Verona, 20 Dicembre 2013.

Marco Caliari _____

Simone Zuccher _____

LICEO STATALE "ENRICO MEDI"

CON INDIRIZZI: *SCIENTIFICO – SCIENTIFICO SCIENZE APPLICATE - LINGUISTICO – SCIENZE UMANE – ECONOMICO SOCIALE - CLASSICO*

Sede: VIA MAGENTA, 7/A - 37069 VILLAFRANCA di VERONA - Tel. 045.7902067 Fax : 045.6300817

e-mail sede: info@liceomedi.com - Preside : preside@liceomedi.com

Sito http://www.liceomedi.com

C.F. 80014060232 Codice meccanografico VRPS06000L

Piano Lauree Scientifiche 2013-2014

Verbale del terzo incontro con gli studenti: Martedì 18 Dicembre 2013, ore 13:45-16:45

Aritmetica modulo N (esempio dell'orologio), proprietà fondamentali. Esercizi preliminari (senza ulteriori spiegazioni): calcolo degli opposti e degli inversi in Z_{24}. Algoritmo di divisione di Euclide (esempi). Identità di Bézout.

Funzione di Eulero (numero di elementi di invertibili in Z_N o, equivalentemente, il numero di elementi coprimi con N (contando anche l'uno). Calcolo empirico della funzione di Eulero per N piccolo: 7 (numero primo), 21 (numero semiprimo, prodotto di due primi) e 24 (numero composto).

Teorema di Eulero (senza dimostrazione) e corollario sull'inverso; verifica per i numeri in Z_{26} (9 ed il suo inverso $9^{11}=3$, che è l'inverso di 9 in quanto il prodotto 9x3=27=26+1). Ma è veramente facile calcolare la funzione di Eulero? In alcuni casi sì: se N è primo (gli elementi coprimi con il numero primo p sono tutti i precedenti p-1); se $N=pq$, con p e q primi, i coprimi con N sono tutti (pq) eccetto i multipli di p, ossia q, e i multipli di q, ossia p, ai quali va aggiunto 1 in quanto il multiplo comune pq è stato tolto 2 volte. Pertanto i coprimi con pq sono $pq-p-q+1=(p-1)(q-1)$. In generale, però, il calcolo della funzione di Eulero è difficile da effettuare perché occorre scomporre N in fattori primi.

Villafranca di Verona, 18 Dicembre 2013.

Marco Caliari _____

Simone Zuccher _____

LICEO STATALE "ENRICO MEDI"

CON INDIRIZZI: *SCIENTIFICO – SCIENTIFICO SCIENZE APPLICATE - LINGUISTICO – SCIENZE UMANE – ECONOMICO SOCIALE - CLASSICO*

Sede: VIA MAGENTA, 7/A - 37069 VILLAFRANCA di VERONA - Tel. 045.7902067 Fax : 045.6300817

e-mail sede: info@liceomedi.com - Preside : preside@liceomedi.com

Sito http://www.liceomedi.com

C.F. 80014060232 Codice meccanografico VRPS06000L

Piano Lauree Scientifiche 2013-2014

Verbale del quarto incontro con gli studenti: Venerdì 11 Gennaio 2014, ore 13:45-16:45

Spiegazione del funzionamento dell'algoritmo RSA utilizzando l'esempio di Alice che deve mandare un messaggio a Bob. Prima di tutto il ricevente, ossia Bob, deve mettere a disposizione di chiunque voglia mandargli un messaggio la sua chiave pubblica, che è usata dal mittente per criptare il messaggio, mentre la chiave privata del ricevente rimane nota a lui solo. Bob deve quindi generare le due chiavi secondo i seguenti passi:

1. Scegliamo p=11, q=7 e calcoliamo N=pq=77.
2. Calcoliamo la funzione di Eulero per N=77, che vale 60.
3. Scegliamo un numero e, coprimo con la funzione di Eulero e minore di essa, per esempio e=7.
4. Calcoliamo d, inverso di e in modulo 60, ossia in modulo la funzione di Eulero, che è 43.
5. La chiave pubblica è la coppia (e,N)=(7,77)
6. La chiave privata è la coppia (d,N)=(43,77)

Supponiamo che Alice voglia mandare, in modo cifrato con l'algoritmo RSA, il numero m=3. Per farlo utilizza la chiave pubblica di Bob che è la coppia (e,N)=(7,77) calcolando il numero cifrato c come $c = m^e \bmod N = 31$. Bob riceve c=31 e, utilizzando la propria chiave privata calcola il numero $x = c^d \bmod N = 3$, che è proprio il numero m che Alice voleva mandargli.

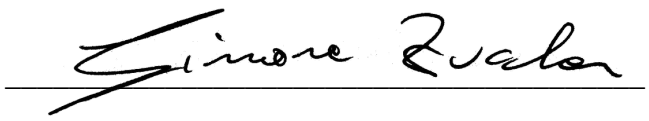
Calcolo dell'inverso mediante algoritmo di Euclide (implementazione in Excel).

Fattorizzazione di una chiave a 18 bit: scomporre in Excel 161219 (613x263) senza suggerimento alcuno.

Stima di Hadamard per il numero di numeri primi, esempio dei numeri primi a 64 bit.

Villafranca di Verona, 11 Gennaio 2014.

Marco Caliari 

Simone Zuccher 

LICEO STATALE "ENRICO MEDI"

CON INDIRIZZI: *SCIENTIFICO – SCIENTIFICO SCIENZE APPLICATE - LINGUISTICO – SCIENZE UMANE – ECONOMICO SOCIALE - CLASSICO*

Sede: VIA MAGENTA, 7/A - 37069 VILLAFRANCA di VERONA - Tel. 045.7902067 Fax : 045.6300817

e-mail sede: info@liceomedi.com - Preside : preside@liceomedi.com

Sito http://www.liceomedi.com

C.F. 80014060232 Codice meccanografico VRPS06000L

Piano Lauree Scientifiche 2013-2014

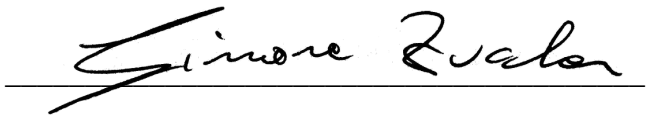
Verbale del quinto incontro con gli studenti: Mercoledì 16 Gennaio 2014, ore 13:45-16:45

Ripasso dell'algoritmo RSA. Dopo il ripasso, gli studenti vengono divisi in due gruppi, ciascuno dei quali genera una coppia di chiavi a partire da due numeri primi a 10 bit, fornisce all'altro gruppo la chiave pubblica, invia all'altro gruppo un messaggio criptato e riceve a sua volta un messaggio da decriptare.

Attacco all'RSA: viene intercettato il messaggio criptato c, e si conosce la chiava pubblica $(e,N)=(7,77)$. Il problema si riduce a calcolare i due numeri primi che hanno per prodotto 77. Se essi sono sufficientemente grandi, ci si fida che l'attacco richieda troppo tempo. Evidentemente, le due chiavi sono generate localmente dal ricevente. Firma digitale.

Villafranca di Verona, 16 Gennaio 2014.

Marco Caliari 

Simone Zuccher 

LICEO STATALE "ENRICO MEDI"

CON INDIRIZZI: *SCIENTIFICO – SCIENTIFICO SCIENZE APPLICATE - LINGUISTICO – SCIENZE UMANE – ECONOMICO SOCIALE - CLASSICO*

Sede: VIA MAGENTA, 7/A - 37069 VILLAFRANCA di VERONA - Tel. 045.7902067 Fax : 045.6300817

e-mail sede: info@liceomedi.com - Preside : preside@liceomedi.com

Sito http://www.liceomedi.com

C.F. 80014060232 Codice meccanografico VRPS06000L

Piano Lauree Scientifiche 2013-2014

Verbale del sesto incontro con gli studenti: Martedì 22 Gennaio 2014, ore 13:45-16:45

Nella prima parte dell'incontro il dott. Marco Caliari descrive alcune problematiche numeriche insite nei sistemi di calcolo come Excel (overflow, troncamento, ecc.). Segue una breve illustrazione dei corsi di laurea afferenti all'area Scienze e Ingegneria dell'universita` di Verona. Infine, viene lasciato spazio alla condivisione dell'esperienza fatta e ai commenti da parte degli studenti sull'utilità o meno del progetto.

Gli studenti confermano il loro interesse verso iniziative come il Progetto "Piano Lauree Scientifiche" in quanto ha permesso loro di rendersi conto di come venga davvero utilizzata la matematica per la risoluzione di problemi pratici ai quali prima non avrebbero mai pensato. A differenza degli altri anni, viene apprezzato il fatto che il progetto sia stato proposto durante i mesi di novembre e dicembre, durante i quali i ragazzi sono meno impegnati con altri progetti pomeridiani. Quasi unanimemente viene caldeggiato dagli studenti di ridurre la durata del singolo incontro da tre a due ore ciascuno. Nel complesso, comunque, gli studenti esprimo apprezzamento ed entusiasmo nei confronti dell'iniziativa.

Villafranca di Verona, 22 Gennaio 2014.

Marco Caliari 

Simone Zuccher