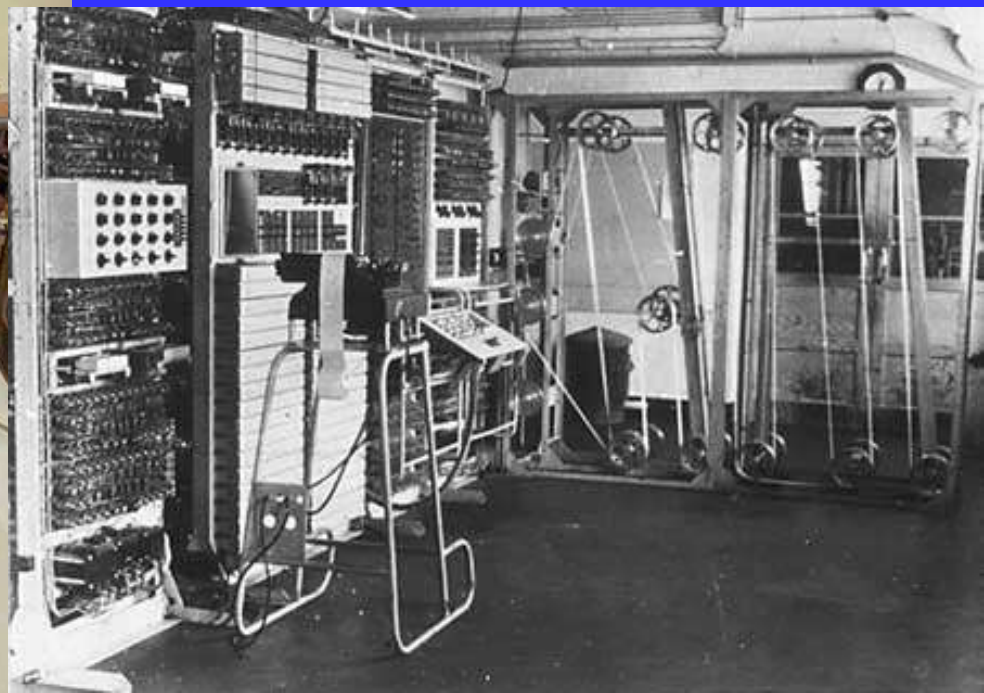
bruno:versione breve

Introduzione alla Crittografia

V1.1 BC 12/2008-12/2010

Enigma

Colossus



Cifratura/crittografia

- “Giuseppe parla in maniera *criptica*” ovvero “non si capisce nulla di ciò che dice”
- La *cripta* della chiesa…

Etimologia (da etimo.it)

cripta e **critta** = *lat.* CRÝPTA dal *gr.* CRÝPTÊ *luogo coperto, nascosto*, e questo da KRÝPTÔ *copro, nascondo* (cfr. *Grotta*).

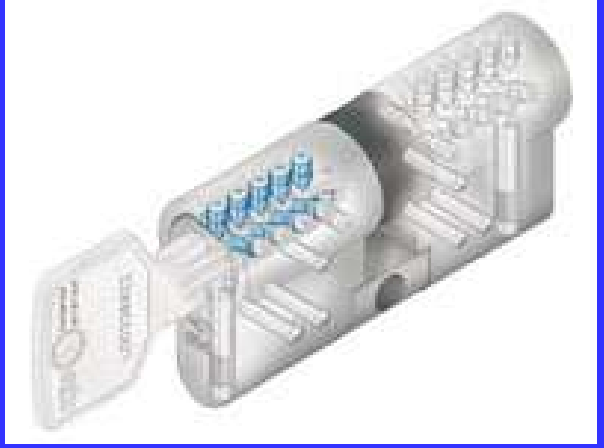
In origine con questo nome si designò Una specie di stretta galleria a terreno, chiusa ai due lati da muro, che riceveva luce da una fila di finestre aperte da una delle parti laterali e che i Romani dissero propr. CRYPTO-PÒRTICUS. Tali gallerie si costruivano per comodo della popolazione, che quivi conveniva a geniale ritrovo, quando il caldo o le intemperie rendevano desiderabile lo stare al coperto. Si chiamarono poi CRIPTÆ anche certi loggiati intorno alle ville per tenervi riparati dalla umidità i prodotti dei campi. Più tardi, il vocabolo fu applicato al significato di Passaggio o luogo sotterraneo e finalmente a quello di Volta o cella.

Volta o cella sotterranea specialm. sotto una chiesa, nella quale si seppellisca o si custodiscano sacre reliquie: ed è anche sinonimo di Catacomba. E qui giova notare che quando le basiliche o tribunali furono trasformati in templi cristiani, la parcere sotto la tribuna si cambiò in santuario.

Cfr. *Crittògamo*

bruno: crittografia: da Cryptos (nascosto in greco)

Cifratura:



- Rendere incomprensibile un messaggio
- in modo che **solo chi sa** come decifrarlo…
- ...possa comprenderlo
- il messaggio può essere intercettato…
- …ma, senza metodo di decifrazione …

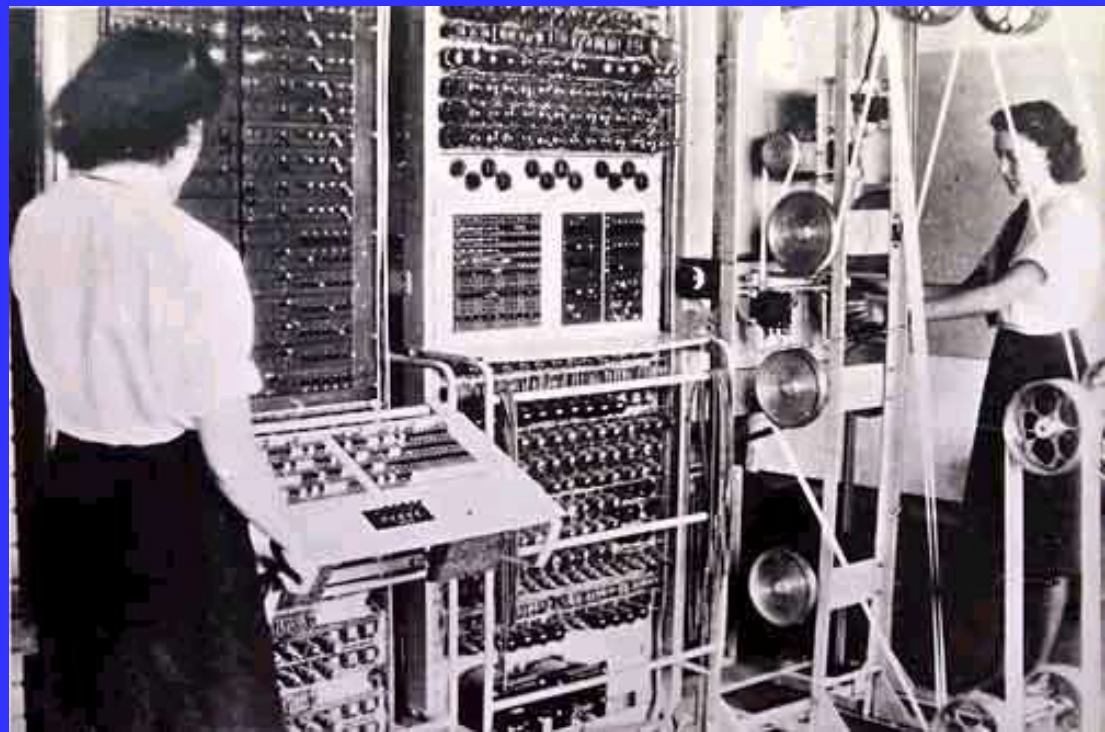
De-cifratura

- Testo in chiaro $\xrightarrow{\text{cifratura}}$ testocifrato $\xrightarrow{\text{decifratura}}$ Testo in chiaro
- La **decifrazione** NON deve essere ambigua

bruno: le guerre vengono vinte anche grazie alla crittografia

Crittografia: utilizzi

- Militare
- civile (spionaggio industriale)
- privato (conti bancari, informazioni riservate)
- Internet
- Cryptofonini



HOW IT WORKS

1 INTERCEPTION German message intercepted by Allied listening post and converted into tape with punched holes representing letters

2 LOADING Tape made into a loop which is threaded around reels in a frame known as a bedstead

3 READING Spinning at 30mph, tape passes beneath optical reader - wartime equivalent of a modern CD drive.

4 ANALYSING Colossus's brain - the equivalent of a modern hard drive - uses statistical analysis to search for patterns

5 DECODING Operators monitor these patterns seeking to isolate the encrypted message. Lights indicate quality of matches

6 OUTPUT Message unscrambled and sent to teleprinter

7 TRANSLATION Printed version is run through another machine which translates it into readable text

FACTFILE

Size: **9ft high, 16ft long, 10ft wide**

Power: **5,500 watts, enough to heat a small flat**

Performance: **Equivalent to modern PC/ laptop** (pictured right)

Esempi: metodo di (de)cifratura

bruno: qui non c'e' chiave, per decifrare basta conoscere la *regola* che è sempre la stessa (rischioso)

- Trasposizione dei caratteri (tutti!) a coppie
  - Ciao Sophia! Diventa
  - iCoaS poih!a
- cifra corrispondente alla posizione nell'alfabeto
  - Ciao Sophia! Diventa
  - 3,9,1,13,?,17,13,14.8,9,1,?

bruno: per lo spazio ed il ! come faccio? E le maiuscole/minuscole?

Esempi II

bruno: più la chiave è lunga più è sicura

bruno:serve conoscere la chiave che può/deve ovviamente cambiare

- Chiave di tre cifre (es: 132)
- traslo verso destra nell'alfabeto la prima lettera di 1, la seconda di tre posizioni e la terza di 2 poi nuovamente di 1 etc.
- Ciao Sophia! Diventa
- Dnc?Trrinc?

bruno: devo traslare anche lo spazio ed il !

Abcdefghilmnopqrstuvz

abcdefghijklmnopqrstuvwxyz !?

Decifrazione con chiave

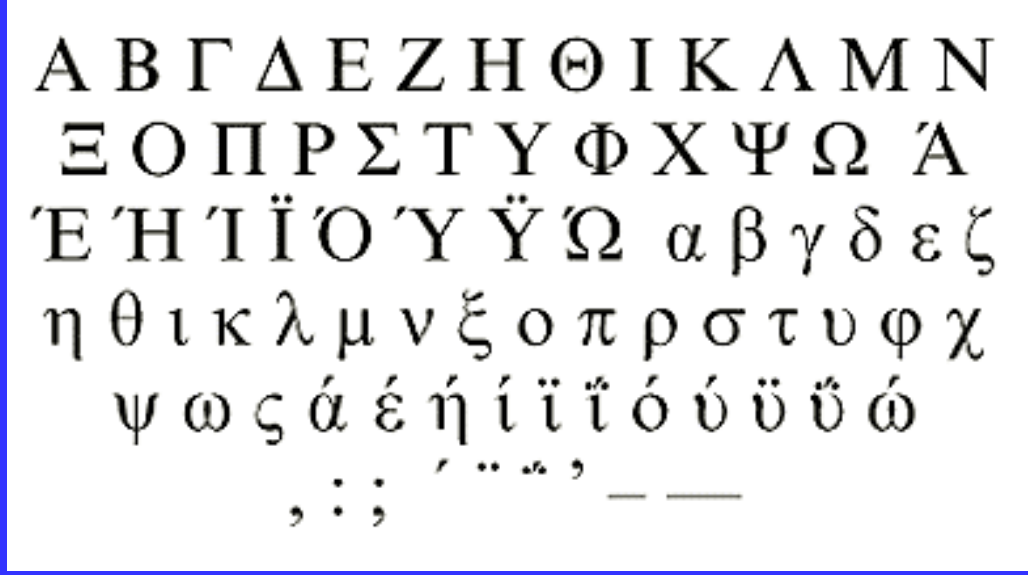
- Per potere decifrare devo conoscere:
- La regola di decifrazione (tornare indietro nell'alfabeto di n posizioni)…
- … e … la CHIAVE (132)
- La chiave può cambiare, anche frequentemente

Aneddoto cifrato

1 2 — 3 4 5 6 7 2 1 7 .
— 8 2 7 — 9 1 3 2 10 5 7
— 11 7 — 1 2 12 1 13 7 13
10 — 8 2 amica 14 4 5 — 14
5 4 2 15 4 5 4 — 1 16 — 15
4 — 4 — 17 7 5 4 — 18 8 7
15 15 5 10 chiacchiere. 15 10 14
10 — 19 4 2 — 13 5 4 2 13
7 — 10 5 4 . — 14 4 5 — 16
1 19 4 5 7 5 9 1 — 15 4 16
16 7 — 16 10 18 8 7 20 4 —
10 9 14 1 13 4 — 20 11 4 —
2 10 2 accennava 7 15 — 7 2
15 7 5 9 4 2 4 . — 11 7 do-
vuto 20 11 1 7 6 7 5 4 — 16
7 — 14 10 16 1 21 1 7 .

Doppia chiave

Esempi III



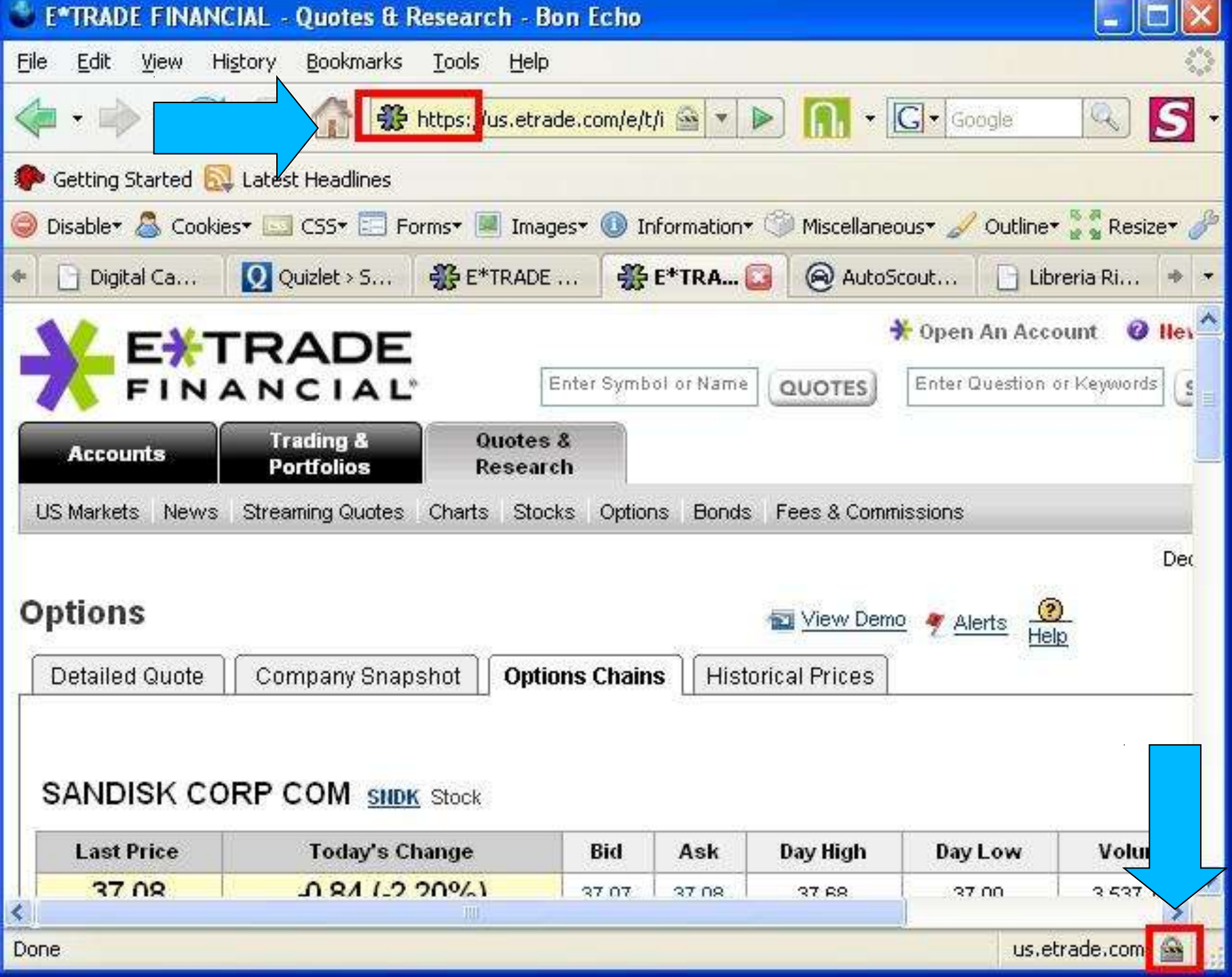
- **Tabella** di **mappatura caratteri** arbitraria
- sostituzione dei simboli di un alfabeto con simboli arbitrari (inventati) o di un altro alfabeto
- “Cosa si capisce qui?” diventa
- ♋□♦♋ ♦♓ ♍♋□♓♦♍♏ ❑◆♓✍

bruno:http Sicuro

SSL: Secure Socket Layer

Crittografia su Internet:

- Https: SSL:
- indispensabile quando su internet “viaggiano”
  - soldi,
  - passwords,
  - informazioni confidenziali
  - posta
  - etc.


E*TRADE FINANCIAL - Quotes & Research - Bon Echo
File Edit View History Bookmarks Tools Help
https://us.etrade.com/e/t/i
Google
Getting Started
Latest Headlines
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize
Digital Ca...
Quizlet > S...
E*TRADE ...
E*TRA...
AutoScout...
Libreria Ri...
E*TRADE FINANCIAL
Open An Account
Enter Symbol or Name
QUOTES
Enter Question or Keywords
Accounts
Trading & Portfolios
Quotes & Research
US Markets News Streaming Quotes Charts Stocks Options Bonds Fees & Commissions
Options
View Demo
Alerts
Help
Detailed Quote
Company Snapshot
Options Chains
Historical Prices
SANDISK CORP COM SNDK Stock
Last Price
Today's Change
Bid
Ask
Day High
Day Low
37.08
-0.84 (-2.20%)
37.07
37.08
37.68
37.00
Done
us.etrade.com


Gmail: Email from Google - Bon Echo
File Edit View History Bookmarks Tools Help
https://www.google.com/a
Google
Getting Started
Latest Headlines
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize
SI - reply....
Gmail:...
Green Car...
Euroseme...
Cleveland ...
ric31_IT.p...
Gmail by Google BETA
Welcome to Gmail
A Google approach to email.
Gmail is a new kind of webmail, built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:
Less spam
Keep unwanted messages out of your inbox with Google's innovative technology
Fast search
Use Google search to find the exact message you want, no matter when it was sent or received.
Sign in to Gmail with your Google Account
Username: bruno.cipolla
Password:
Remember me on this computer.
Sign in
I cannot access my account
Done
www.google.com

Cifratura “industriale - militare”

DES (Data Encryption Standard degli anni '70) chiave (simmetrica) di 56 bit, craccato nel 1999 in una ventina di ore!!

AES (Advanced Encryption Standard del 2001) chiavi di 128, 192 o 256 bit, NON craccabile (per ora)

La NSA prescrive

National Security Agency degli USA

Prescrive

AES 128 o superiori per documenti classificati fino a “Secret”

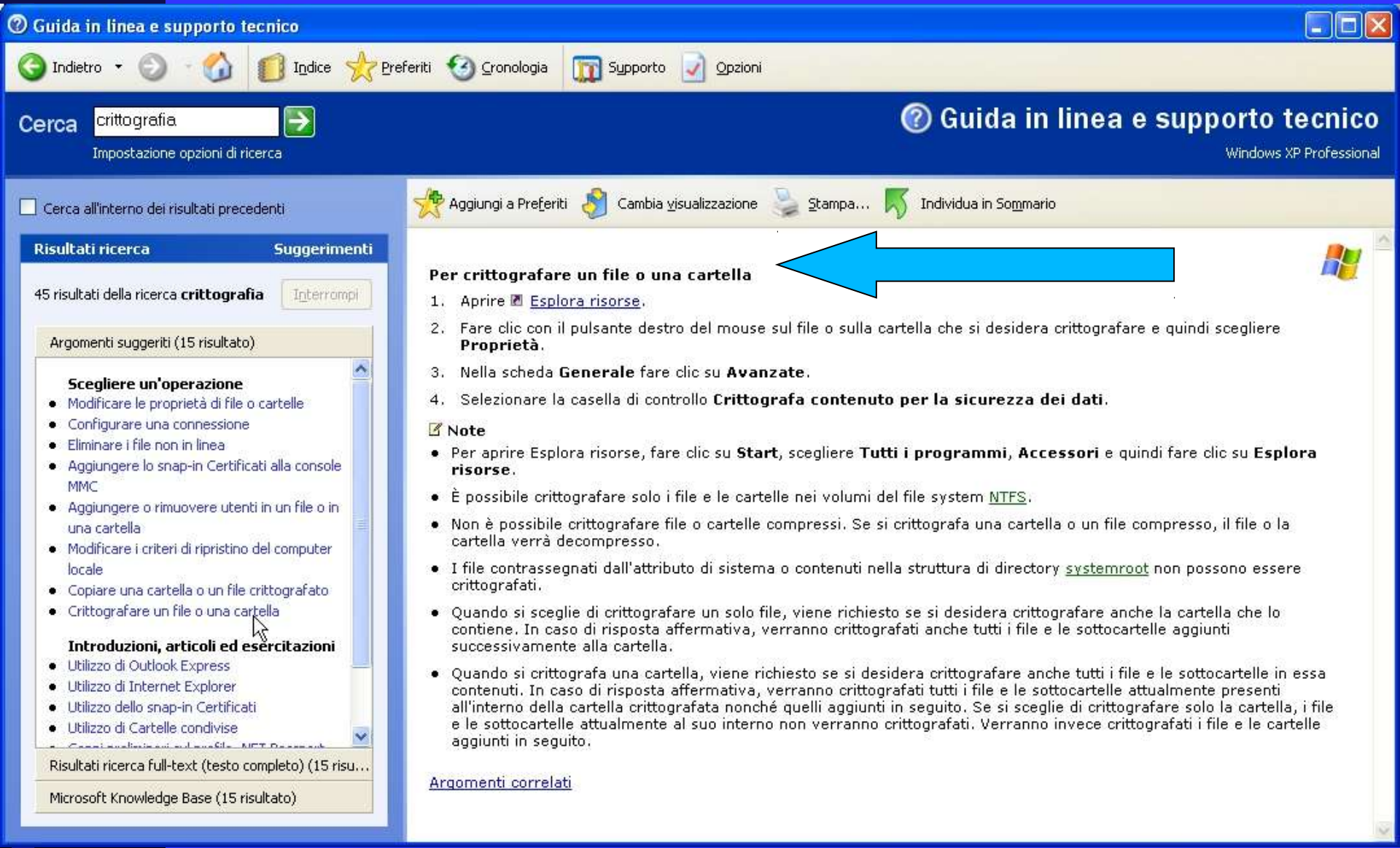
Per TOP Secret minimo 192 o 256 bit.

Classificazione segreti militari e non

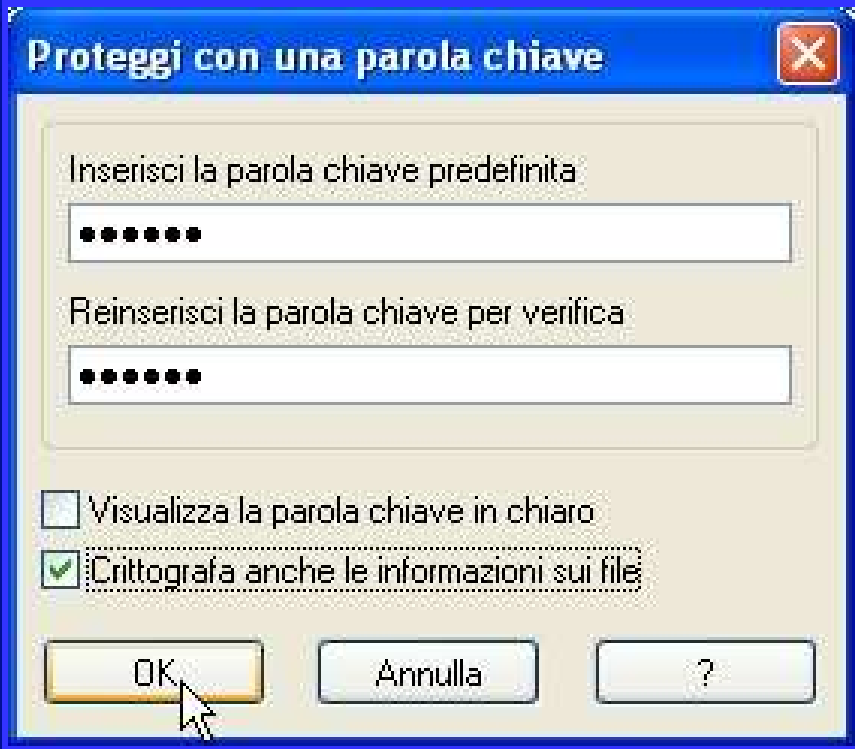
1.1 livelli:

- 1.1.1 Top Secret (TS)
- 1.1.2 Secret
- 1.1.3 Confidential
- 1.1.4 Restricted
- 1.1.5 Unclassified

Crittografia di windows



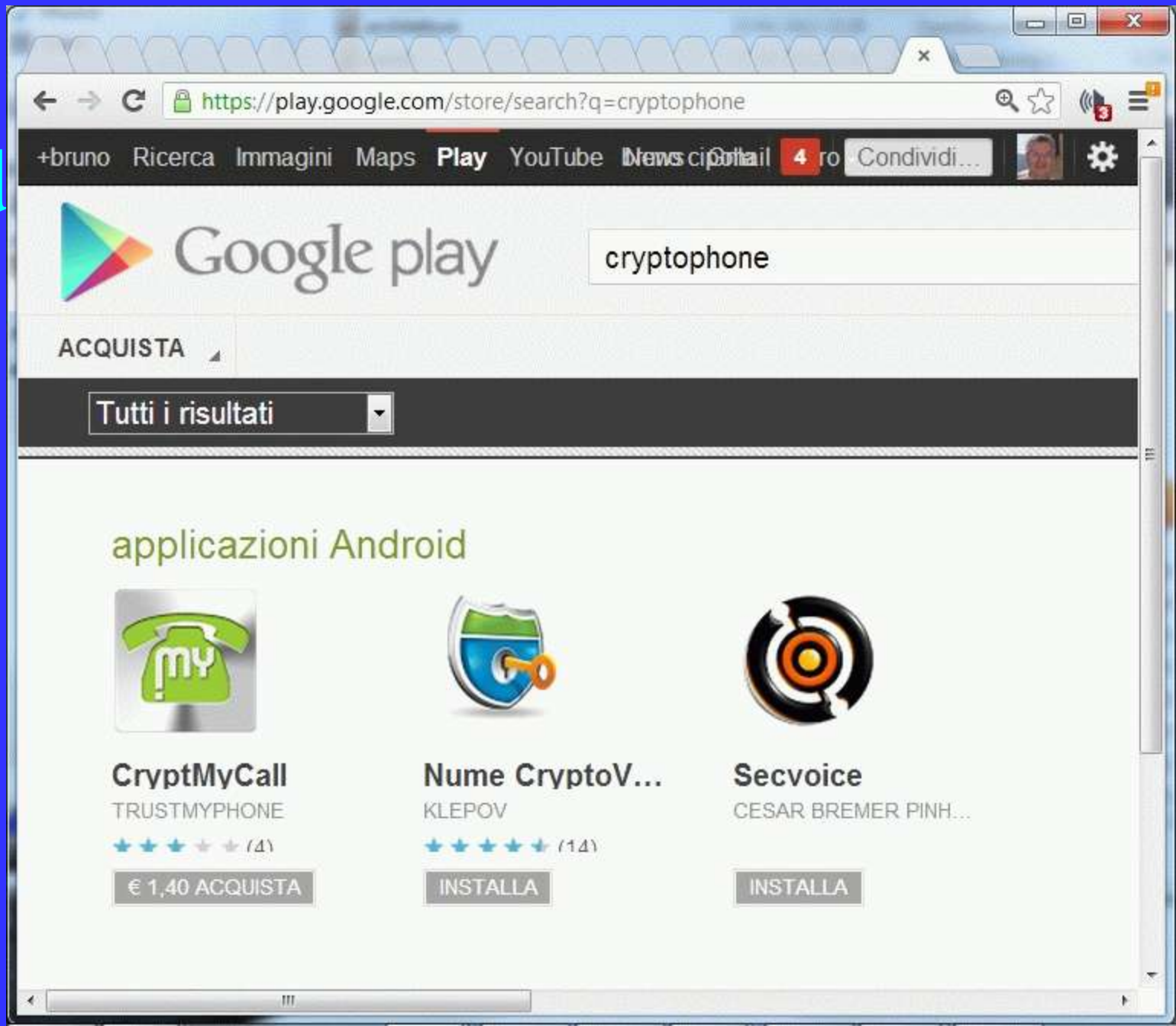
Crittografia sul PC: Winrar



Il Criptofonino

Secondo me dovrebbero essere illegali.

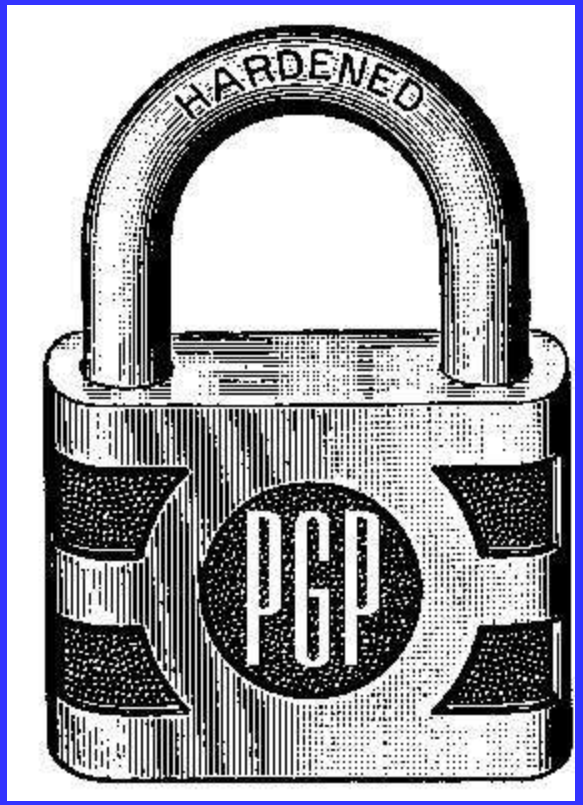
APP per android



bruno:cosa è PGP?

Cifratura

FINE!



Slides extra

Definizioni

- Processare le informazioni in una forma incomprensibile, reversibile, senza perdita di dati
- Solitamente uno ad uno (no compressione)
- Esempio di crittografia analogica: cambiavoce
- Altri servizi:
  - Integrity checking: no tampering
  - Authentication: not an imposter
- Testo in chiaro $\xrightarrow{\text{cifratura}}$ testocifrato $\xrightarrow{\text{decifratura}}$ Testo in chiaro

Computational Difficulty

- Algorithm needs to be efficient.
  - Otherwise only short keys can be used.
- Most schemes can be broken: depends on $$$.
  - E.G. Try all possible keys.
- Longer key is often more secure:
  - Encryption $O(N+1)$.
  - Brute-force cryptanalysis: $O(^{2N+1})$, twice as hard with each additional bit.
- Cryptanalysis tools:
  - Special-purpose hardware.
  - Parallel machines.
  - Internet coarse-grain parallelism.

Secret Key vs. Secret Algorithm

- Secret algorithm: additional hurdle
- Hard to keep secret if used widely:
  - Reverse engineering, social engineering
- Commercial: published
  - Wide review, trust
- Military: avoid giving enemy good ideas

Alcuni Schemi Triviali

- Cifratura di Giulio Cesare: sostituzione simboli:
  - A → D, B → E
- Captain Midnight Secret Decoder rings:
  - shift variable by *n*: IBM → HAL, or :
    - (letter + offset) mod 26
  - only 26 possible ways of secret coding.
- Cifratura Monoalfabetica:
  - mappatura arbitraria di una lettera su un'altra (tabella)
  - 26!, approssimativamente 4×10^{26}
  - analisi statistica delle frequenze delle lettere
- One-time pad
  - A random sequence of 0's and 1's XORed to plaintext

La Crittanalisi: Breaking an Encryption Scheme

- Ciphertext only:
  - Exhaustive search until “recognizable plaintext”
  - Need enough ciphertext
- Known plaintext:
  - Secret may be revealed (by spy, time), thus <ciphertext, plaintext> pair is obtained
  - Great for monoalphabetic ciphers
- Chosen plaintext:
  - Choose text, get encrypted
  - Useful if limited set of messages

Models for Evaluating Security

- Unconditional security (perfect secrecy)
  - Uncertainty/entropy $H(p)=H(p|c)$
- Complexity-theoretic security
- Provable security
  - As difficult to break as solving well-known and *supposedly* difficult problem
- Computational security
- Ad hoc security

Brute Force Attacks

- Number of encryption/sec: 1 million to 1 billion/sec
- 56-bit key broken in 1 week with 120,000 processors ($6.7m)
- 56-bit key broken in 1 month with 28,000 processors ($1.6m)
- 64-bit key broken in 1 week with 3.1×10^7 processors ($1.7b)
- 128-bit key broken in 1 week with 5.6×10^{26} processors

Tipi di Crittografia

- Funzione Hash: nessuna chiave
- Crittografia con chiave segreta: una chiave
- Crittografia con chiave pubblica: due chiavi - pubblica, privata

Crittografia con chiave segreta

- La setssa chiave viene usata per cifrare e decifrare
  - Crittografia Simmetrica
- Ciphertext approximately the same length as plaintext
- Substitution codes, DES, IDEA
- Message transmission:
  - Agree on key (but how?)
  - Communicate over insecure channel
- Secure storage: *crypt*

Secret Key Cryptography (Cont'd)

- Strong authentication: prove knowledge of key without revealing it:
  - Send challenge r, verify the returned encrypted $\{r\}$
  - Fred can obtain chosen plaintext, cihpertext pairs
    - Challenge should chosen from a large pool
- Integrity check: fixed-length checksum for message
  - Send MIC along with the message

Crittografia con chiave pubblica

- Crittografia Asimmetrica
- Inventata nel 1975
- Due chiavi: privata (*d*), pubblica (*e*)
  - Cifratura: chiave pubblica; Decifratura: chiave privata
  - Signing: private key; Verification: public key
- Much slower than secret key cryptography

Public Key Cryptography (Cont'd)

- Data transmission:
  - Alice encrypts m_a using e_B, Bob decrypts to m_a using d_b.
- Storage:
  - Can create a safety copy: using public key of trusted person.
- Authentication:
  - No need to store secrets, only need *public* keys.
  - Secret key cryptography: need to share *secret* key for every person to communicate with.

Public Key Cryptography (Cont'd)

- Digital signatures
  - Encrypt *hash* $h(m)$ with private key
    - Authorship
    - Integrity
    - Non-repudiation: can't do with secret key cryptography

Hash Algorithms

- Message digests, one-way transformations
- Length of $h(m)$ much shorter then length of m
- Usually fixed lengths: 48-128 bits
- Easy to compute $h(m)$
- Given $h(m)$, no easy way to find m
- Computationally infeasible to find m_1, m_2 s.t. $h(m_1) = h(m_2)$
- Example: $(m+c)^2$, take middle n digits

Hash Algorithms (Cont'd)

- Password hashing
  - Doesn't need to know password to verify it
  - Store $h(p+s)$, s (salt), and compare it with the user-entered p
  - Salt makes dictionary attack less convenient
- Message integrity
  - Agree on a password p
  - Compute $h(p|m)$ and send with m
  - Doesn't require encryption algorithm, so the technology is exportable