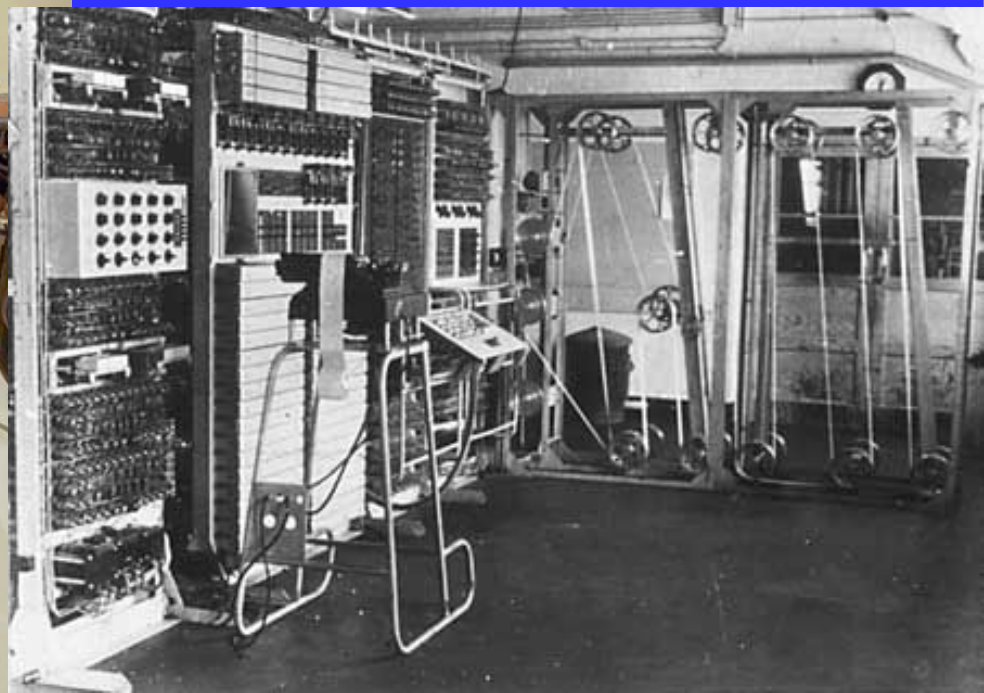
bruno:versione breve

Introduzione alla Crittografia

BC 12/2007

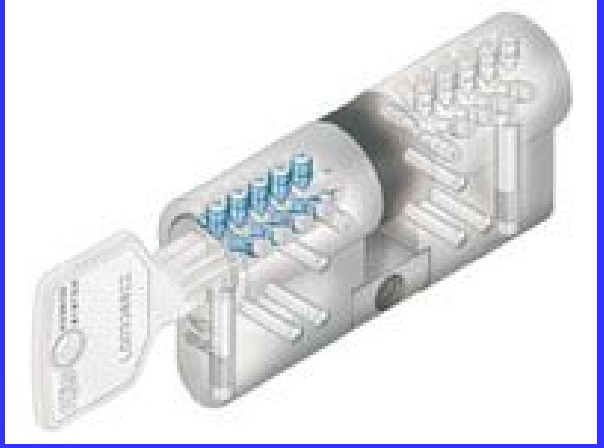
Enigma

Colossus



bruno: crittografia: da Cryptos (nascosto in greco)

Cifratura:

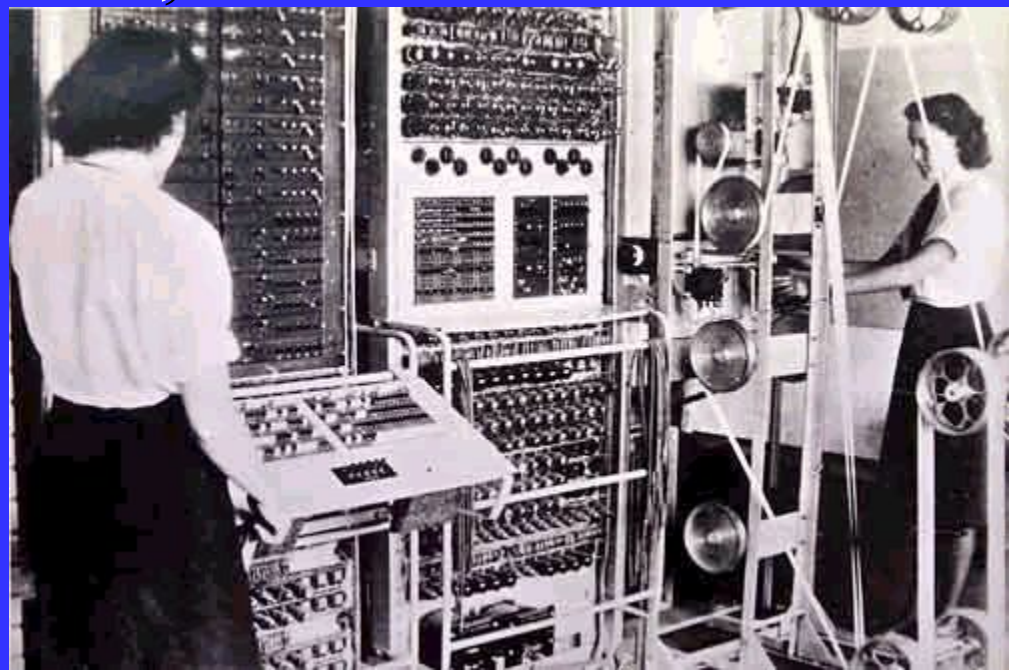


- Rendere incomprensibile un messaggio
- in modo che **solo chi sa** come decifrarlo…
- …possa comprenderlo
- il messaggio può essere intercettato…
- …ma, senza chiave…
- La **decifrazione** NON deve essere ambigua

bruno: le guerre vengono vinte anche grazie alla crittografia

Crittografia: utilizzi

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



esempi

- 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: qui non c'e' chiave, basta sapere la regola che è sempre la stessa

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

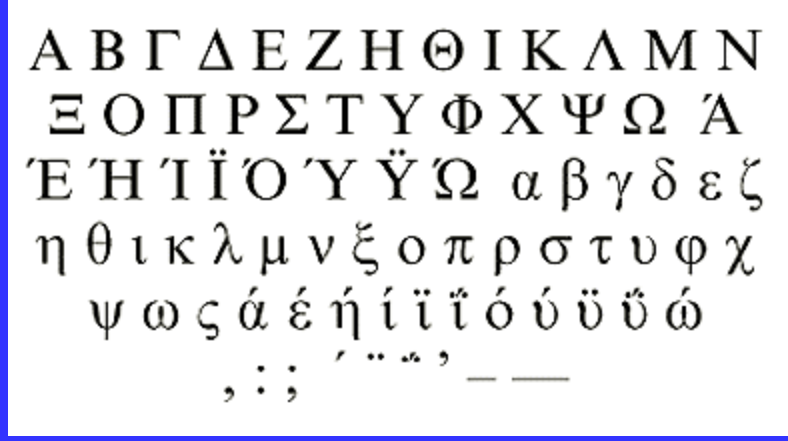
- Chiave di tre cifre (es: 132)
- traslo verso destra la prima lettera di 1, la seconda di tre posizioni e la terza di 2 poi nuovamente di 1 etc.
- Ciao Sophia! Diventa
- Dnc?Trrinc?

bruno: devo traslare anche lo spazio ed il !

Abcdefghilmnopqrstuvz

abcdefghijklmnopqrstuvwxyz !?

Esempi III



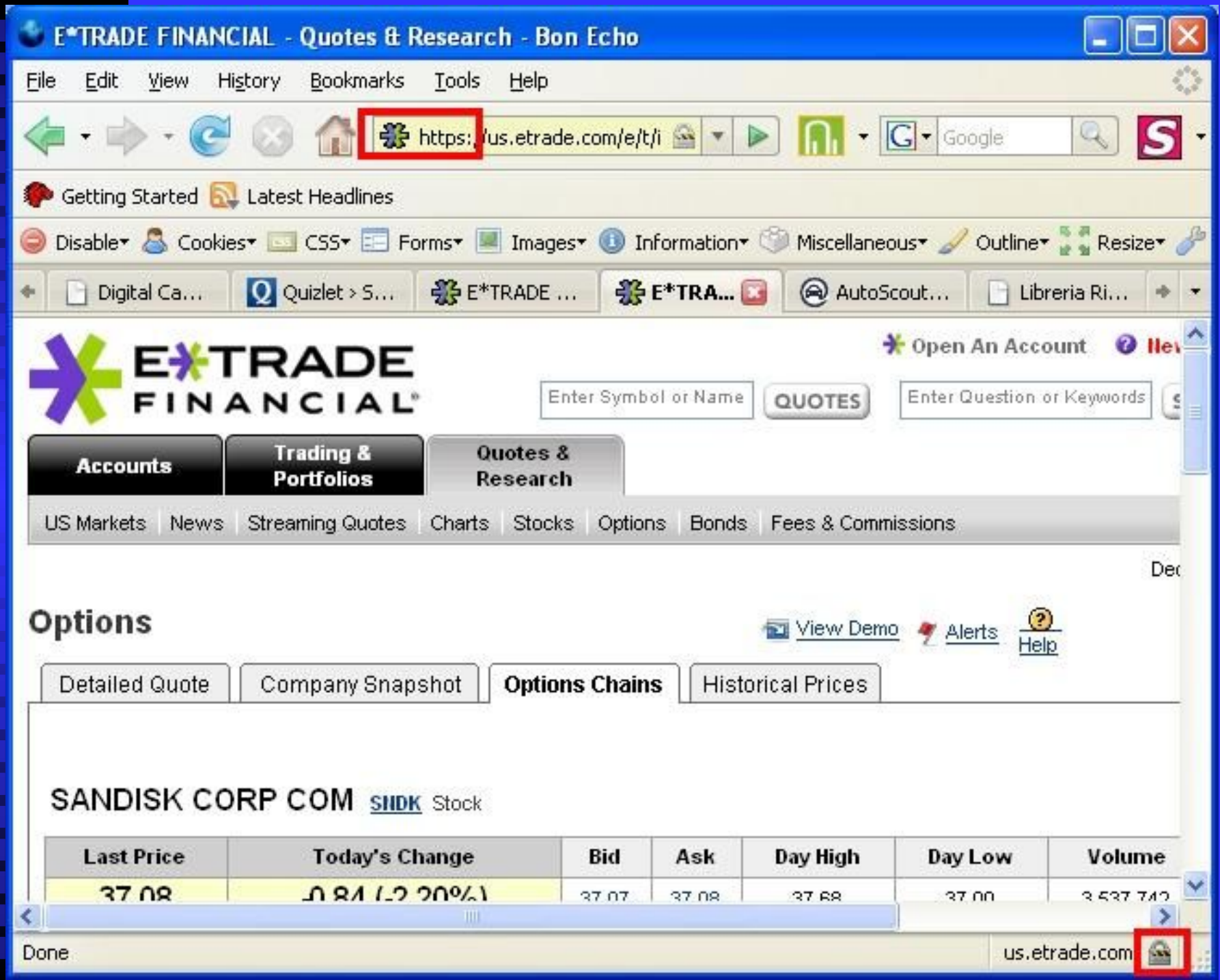
- **Tabella** di **mappatura caratteri** arbitraria
- sostituzione dei simboli di un alfabeto con simboli arbitrari (inventati) o di un altro alfabeto

bruno:http Sicuro

SSL: Secure Socket Layer

Internet:

- Https: SSL:
- indispensabile quando “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
Volume
37.08
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.
Lots of space
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

bruno:cosa è PGP?

Cifratura

FINE!