CryptoKitchen

10 Marzo 2007

Pasta vino e certificati:
la crittografia entra in cucina.

mayhem@recursiva.org
GPG Key ID B88FE057

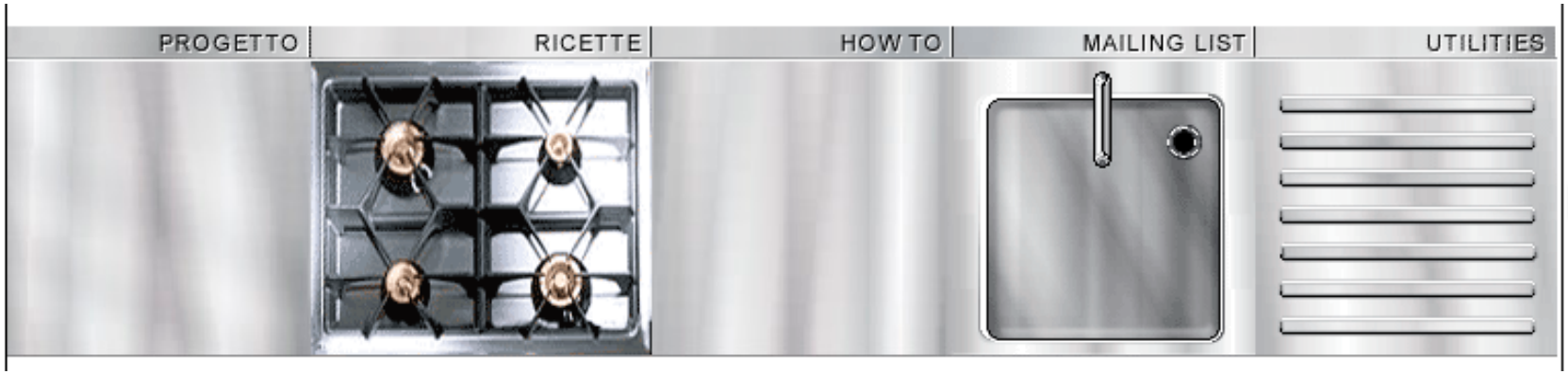
la Chimica

$ whois mayhem

Security Evangelist @ Alba S.T.

Member / Board of Directors:

AIP, AIPSI, CLUSIT, HPP, ILS, IT-ISAC, LUGVR, OPSI, Metro Olografix, No1984.org, OpenBeer/OpenGeeks, Recursiva.org, Sikurezza.org, Spippolatori, VoIPSA.



Benvenuti in cucina!

http://www.cryptokitchen.net/

Il progetto

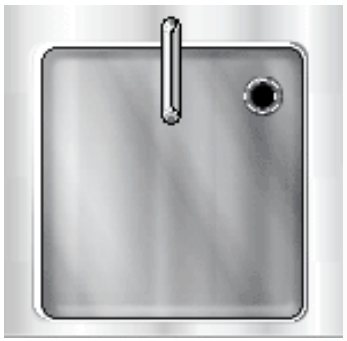
Cryptokitchen nasce dall'idea di un gruppo di donne durante un corso di informatica di base, organizzato per colmare il divario di genere nei confronti delle donne nell'ambito della diffusione delle tecnologie dell'informazione.

http://www.recursiva.org/
mayhem@recursiva.org

Mailing List

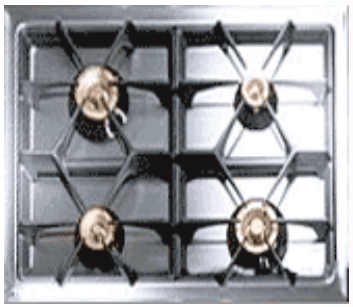
Obiettivi della lista sono: imparare ad usare la crittografia e decriminalizzarne l'uso.

Per questo si scambiano ricette di cucina utilizzando solo mail cifrate.



Le ricette

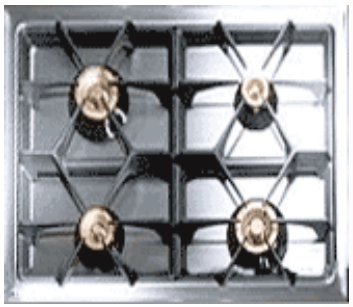
Cryptokitchen è pur sempre una cucina, per quanto particolare. Le ricette sono disponibili sul sito per consultazione. E preparazione :)



http://www.recursiva.org/
mayhem@recursiva.org

Crittografia

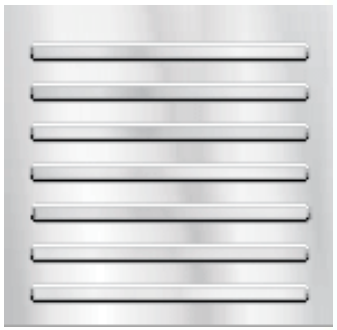
Per invogliare all'uso della crittografia, la spiegazione della preparazione è cifrata, così come è stata scambiata attraverso la mailing list.



http://www.recursiva.org/
mayhem@recursiva.org

Utilities

Che cucina sarebbe senza una completa dotazione di fruste, mestoli, cifratori e decifratori, coltelli, programmi per la posta e robot multifunzione?



http://www.recursiva.org/
mayhem@recursiva.org

Come funziona? - Le chiavi

Come funziona? - Le chiavi

http://www.recursiva.org/
mayhem@recursiva.org

Come funziona? - Le chiavi

Chiave pubblica
della lista

Come funziona? - Le chiavi

Chiave pubblica
della lista

Come funziona? - Le chiavi

Chiave pubblica
della lista

http://www.recursiva.org/
mayhem@recursiva.org

Come funziona? - Le chiavi

Chiave pubblica
della lista

Chiave privata
della lista

Come funziona? - Le chiavi

Chiave pubblica
della lista

Chiave pubblica
della lista

Chiave privata
della lista

http://www.recursiva.org/
mayhem@recursiva.org

Come funziona? - Le chiavi

Chiave pubblica della lista

Chiave privata della lista

Chiave pubblica della lista

Chiave privata della lista

http://www.recursiva.org/
mayhem@recursiva.org

Come funziona? - CypherMix

Un programma automatico decripta la ricetta inviata, “legge” i campi che la compongono e la ri-cripta per la pubblicazione sul sito.

Come funziona? - Le chiavi

Chiave privata della lista

Chiave pubblica della lista

Chiave privata della lista

Chiave pubblica della lista

Chiave privata della lista

http://www.recursiva.org/
mayhem@recursiva.org

Marla rides Furia

-----BEGIN CK RECIPE-----

TTL: Marla rides furia

CAT: 33

ING: 4 porzioni di filetto di cavallo morto in battaglia

1 bottiglia di montenegro

cipolla, sedano, aglio: questo e' quel che taglio

farina, olio d’oliva e.v., burro, sale, pepe: questi vanno sempre

molto ghiaccio, perche' freddo io piaccio

http://www.recursiva.org/
mayhem@recursiva.org

ATT: padella modello ritorno dello jedi, un ampio bicchiere di cristallo, 3 amici carnivori, un grembiulino di pizzo bianco.

PER: 4

TMP: 1 ora scarsa. se dovete prendere il cavallo al laccio potrebbe servire qualche ora piu' del previsto.

DIF: facile, soprattutto se il cavallo non cerca di bersi il montenegro.

PRE:

La ricetta

2. primi | 23. zuppe | Submit

42. Buridda di seppie hackit 04

Dalla cucina di: Spinhacker404

ingredienti: 1 kg tra totani e polipetti puliti, aglio (tantissimo), prezzemolo (tantissimo), quattro pomodori freschi, 1/2 kg patate, vino bianco

attrezzi: pentola capiente, padella, coltello, tagliere

persone: 6

tempo: 00:00:01

difficolta: facil

preparazione: preparare soffritto con prezzemolo e

- **Come la decifro?**

jA0EAwMC0XyPdGXOaZJgycDPNAzHqoDyRX+cmmAOgEUxroEDkAKyJpDsvvzah0Bm
XEPUnyJDi72CcQbxVF56W33IvReoYuzbXeihaWlrQ1/uw82WwFHIg/Pe+F/+mT8x
pSV9Y+24nurnlx7JZDK0HZUFe7H+Ocx2rfmDAfoIC1pSu4v/NStGFeqQkD4lF676
91re8ie8FclB6C56P7+LVznZ6wXCk8kbqtrV64dcMIY6zHFkR9uLgsXJOLdDOXus
RrTX6kfL3WKvcrFMnymRazzhB8dRSzQaxl8773bxBqbkDB+O0Wamzr1z1XhtojuK
3Bi1AUSaZU3EK1VwDSg3cD9s1F4RhgtlGoJS7DL7QEjlSh6bn32RMzn6U/61yd/+
s3ATsdxXh0nPJnHh22vijIAM8ZDDTsUl9F5zHoDisDi3UiTyvWdOWyo9xg74W37O
XP+bQePH3RV6LvuXM7FPmrMddTAnWbo96+lspvJHuxFxqL1BydVD4MeGN/8BS6mo
rETdvAzx2bMdGWMJJfPd/O38sWvhnlZ26PZ6rY+o03/b =In7g

http://www.recursiva.org/
mayhem@recursiva.org

Come si legge?

Usando GPG ed utilizzando come passphrase la prima riga della ricetta.

```
gpg -d preparazione.epl -o sformato_melanzane.txt
Enter passphrase: Pulite le melanzane con cura e tagliatele
```


http://www.recursiva.org/
mayhem@recursiva.org

Present & Future

http://www.recursiva.org/
mayhem@recursiva.org

Present & Future

- ✓ Il progetto ha alti e bassi di vitalità

http://www.recursiva.org/
mayhem@recursiva.org

Present & Future

- ✓ Il progetto ha alti e bassi di vitalità
- ✓ Le persone iscritte sono diverse decine

Present & Future

- ✓ Il progetto ha alti e bassi di vitalità
- ✓ Le persone iscritte sono diverse decine
- ✓ Al momento cyphermix è in manutenzione, quindi non tutte le ricette immesse sono consultabili

http://www.recursiva.org/
mayhem@recursiva.org

Present & Future

- ✓ Il progetto ha alti e bassi di vitalità
- ✓ Le persone iscritte sono diverse decine
- ✓ Al momento cyphermix è in manutenzione, quindi non tutte le ricette immesse sono consultabili
- ✓ Aspettiamo anche la vostra partecipazione!

http://www.recursiva.org/
mayhem@recursiva.org

Domande?

Queste slide sono disponibili su:
http://www.recursiva.org

Per domande o approfondimenti:
mayhem@recursiva.org

la Chimica

Domande?

Grazie per l'attenzione!

Queste slide sono disponibili su:
http://www.recursiva.org

Per domande o approfondimenti:
mayhem@recursiva.org

la Chimica