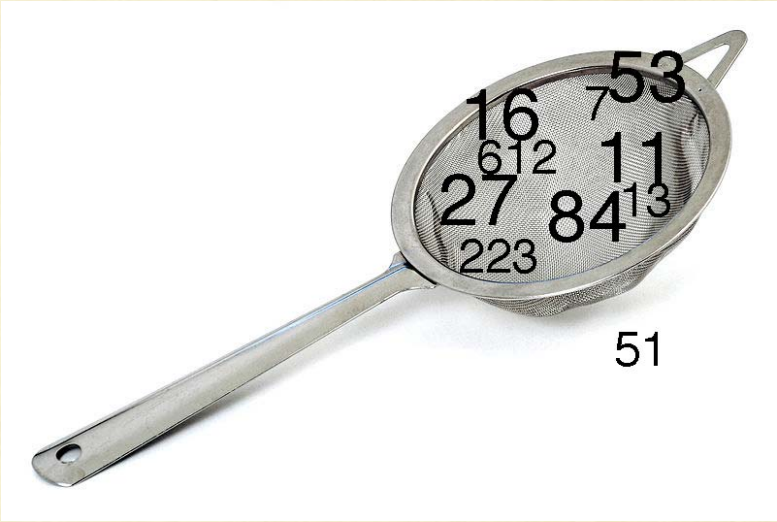
A menu for the Dining Cryptographers

Dic Bolony and Ed I. Blast
A University of Yon Queen Length Clods

ASIACRYPT 2010 Rump Session

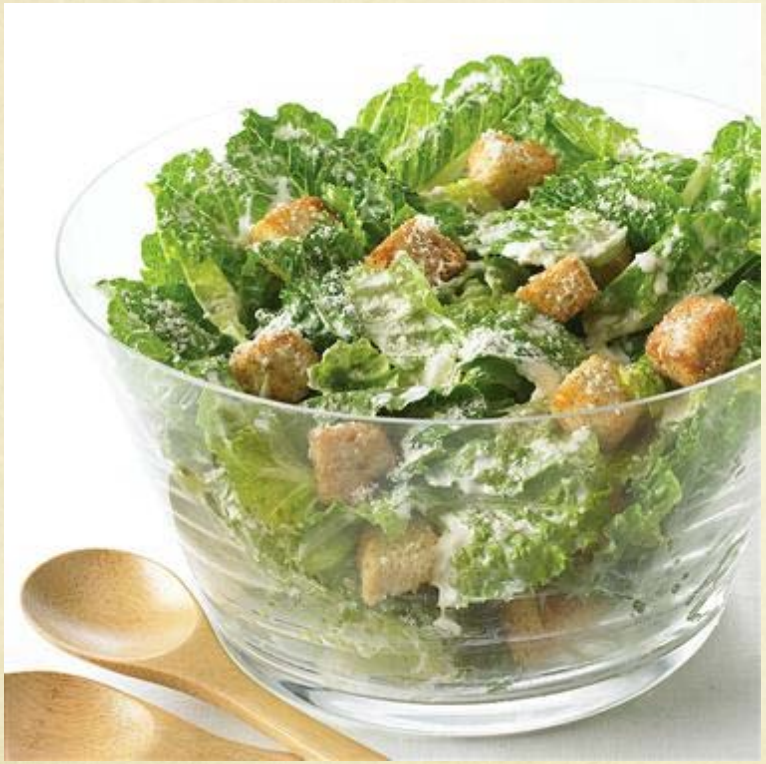
Cooking implements

- Number Field Sieve
- paring knives
- DES in ECB (Electronic-Cookbook) mode
- mix networks
- forking lemma



Salad

- Casear cipher salad

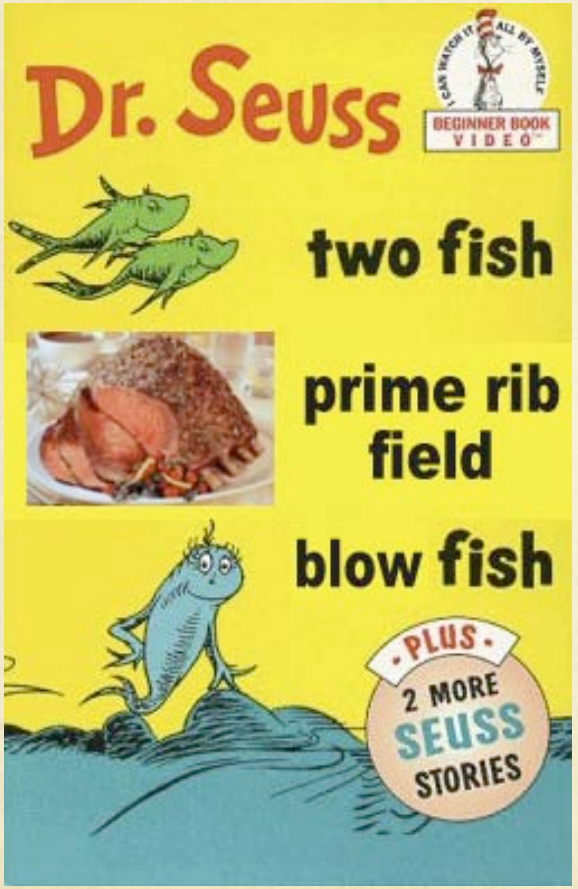


- Garden salad
  - lettuce-based encryption
  - onion-routing
  - pseudoradish
  - olive Euler
  - random seeds
  - unbalanced oil and vinegar
  - add salt

Pasta

- Cannelloni-Krawczyk model
- HMACaroni and cheese
- add a nonce for freshness

Main course



- Twofish
- Prime rib field
- Blowfish

- A meat-in-the-middle attack

Triple-DESsert

- birthday attack cake
- bread pudding protocols
- key lime pie*

- * zero-calorie proof of knowledge

After dinner

- TEA
- orange CRUSH
- abelian grape juice
- MACadamia nut cookies
- cube root beer

$\sqrt[3]{}$

Thank you (and sorry!)

If you thought this talk was not funny enough, please be sure to name your next cryptographic algorithm/protocol after a food or drink.