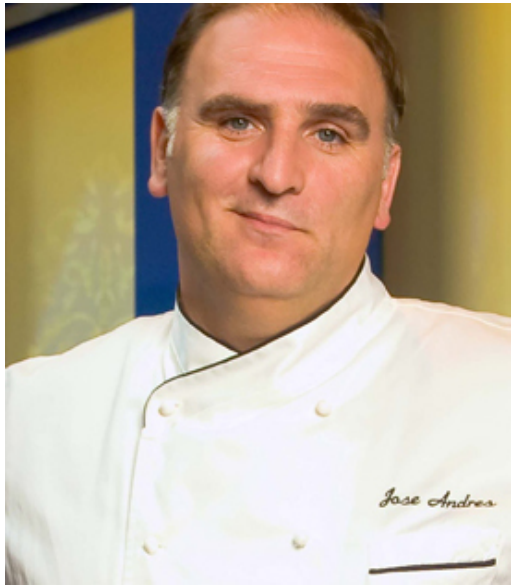


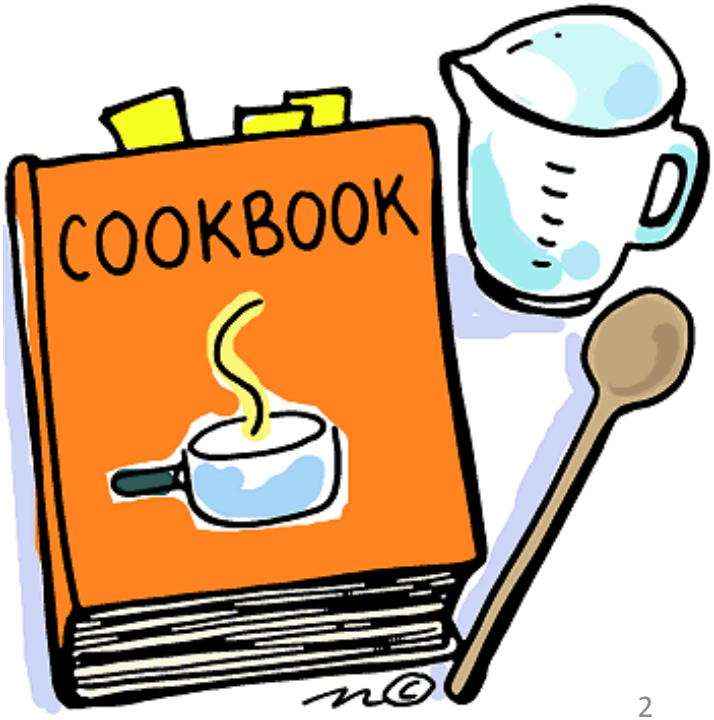
Cooking with JOSE

Matt Miller

IETF 89 - London

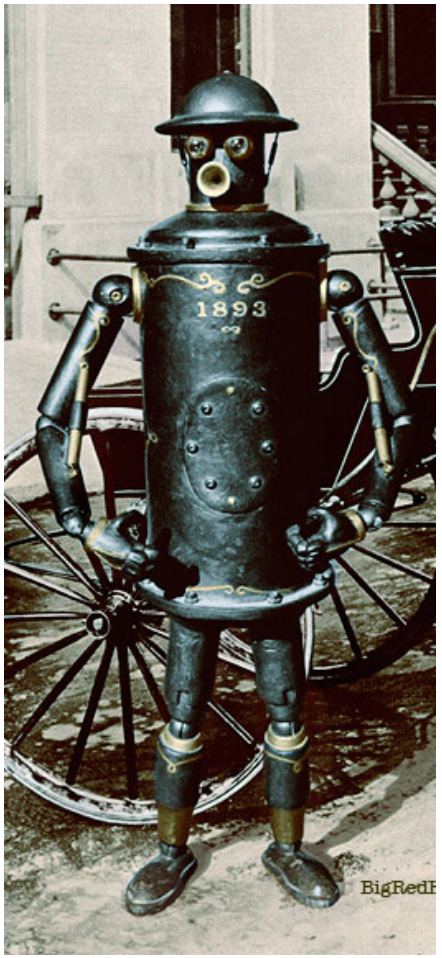
The Basic Premise

- Examples of how to Sign
  - Various inputs
  - Various outputs
- Examples of how to Encrypt
  - Various inputs
  - Various outputs



draft-ietf-jose-cookbook

- 75+ pages of examples
  - 80+ with boilerplate
- All recipes follow the same style
  - Inputs
  - Generated factors
  - Operations
  - Outputs (Compact + JSON)



Signature Recipes

All recipes use the same payload

- Different algorithms
- Different key types
- Different header protection levels
- Detached
- Multiple signatures

Encryption Recipes

(Almost) all recipes use the same plaintext

- Different key algorithms
- Different content algorithms
- Different key types
- Different header protection levels
- Explicit AAD
- Compression
- Multiple Recipients

Next Steps

- Update to match latest JW*
- Reviews!