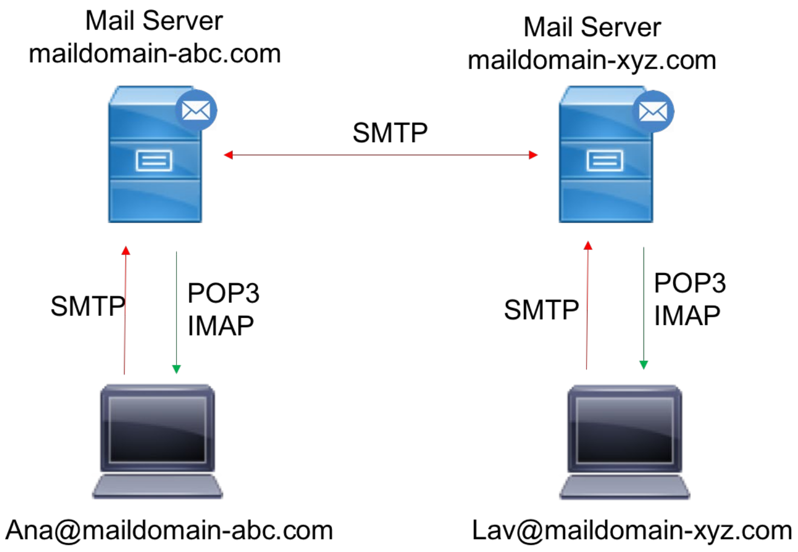
E-mail Security



Spam Filtering

- Keyword matching.
  - ➢ Check through blacklist of words.
  - ➢ Easily bypasses by spammer adding spaces, punctuation, substitute letters

- Bayesian Filtering.
  - ➢ Uses machine learning to distinguish between Spam and normal e-mail
  - ➢ Needs to be “trained”

- ALPACAS: **A** **L**arge-scale, **P**rivacy-**A**ware **C**ollaborative **A**ntispam **S**ystem.
  - ➢ Identifies “fingerprints” of spam e-mail based on style, layout
  - ➢ Changes on content, obfuscation don’t trick it

Pretty Good Privacy (PGP)

- E-mail messages are:
  - ➢ Digitally signed
  - ➢ Encrypted
  - ➢ Hashed

- Uses Web of Trust (instead of CA) to verify public keys:
  - ➢ Based on reputation of public keys
  - ➢ Open source version is GPG (Gnu Privacy Guard)

E-mail Authentication

- Authentication of sending user (client) relies on public key crypto:
  - ➢ Everyone must have a certificate
  - ➢ Not used much

- Authentication of the organization:
  - ➢ Uses certificate embedded in gateway (e.g. Astaro appliance)
  - ➢ Easier to use, so more common

Sender Policy Framework (SPF)

- SPF field in DNS record used to authenticate e-mail server.
  - ➢ Easy to spoof.
  - ➢ Does not check message integrity.
  - ➢ No privacy (encryption).
  - ➢ Does not support mail forwarding.

- Some adoption, but not commonplace