What is greylisting?

- How to detect and filter spam?
  - Many Anti-spam techniques:
    - Content analysis
    - IP reputation
    - [...]
What if sending e-mail fails?

• Legitimate e-mail senders:
  - Retry for 4 days in 30min interval

• Spamers:
  - Too costly to track status and retry
Normal SMTP traffic

> HELO somedomain.com
<- 250 Hello somedomain.com
-> MAIL FROM: <sender@somedomain.com>

<- 250 2.1.0 Sender ok
-> RCPT TO: <recipient@otherdomain.com>
<- 250 2.1.5 Recipient ok
-> DATA
<- 354 Enter mail
...  
<- 250 2.0.0 Message accepted for delivery
Greylisted SMTP traffic

> HELO somedomain.com
<- 250 Hello somedomain.com
-> MAIL FROM: <sender@somedomain.com>
<- 250 2.1.0 Sender ok
-> RCPT TO: <recipient@otherdomain.com>
<- 250 2.1.5 Recipient ok
-> DATA
<- 451 4.7.1 Please try again later
Pros

- Catches > 90% spammers
- Non CPU intensive

Cons

- Delay in delivery
Challenge
Solution