Making Anonymous Communication

Paul Syverson

Center for High Assurance Computer Systems

Naval Research Laboratory

http://www.onion-router.net/

syverson@itd.nrl.navy.mil

Presented at the National Science Foundation,

June 8, 2004

Talk Outline

- Motivation: Why anonymous communication?
  - Personal privacy
  - Corporate and governmental security
  - Note: Anonymous comm. = Traffic analysis resistant comm.
- Characterizing anonymity: Properties and Types
- Mixes and proxies: Anonymity building blocks
- Onion Routing: Lower latency, Higher Security
- Features of Tor: 2nd Generation Onion Routing
- Hidden Servers and Rendezvous Points
- Summary and Future Work

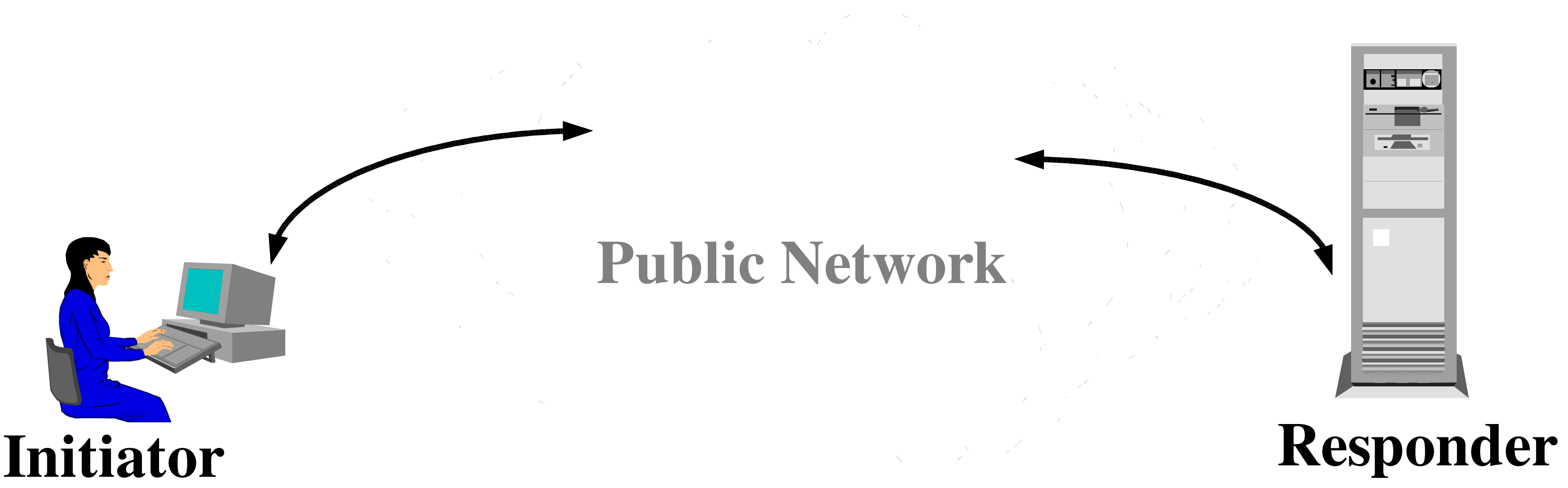
Credits

- Some slides on mixes cribbed from Ari Juels (with permission)
- Original Onion Routing concept, design, research, patent, etc.
  - with David Goldschlag and Michael Reed
- Tor, second generation Onion Routing
  - with Roger Dingledine and Nick Mathewson

- Numerous research predecessors and contemporaries
- Lots of volunteers contributing to open source Tor code, running nodes, etc.

Public Networks are Vulnerable to Traffic Analysis

- In a Public Network (Internet):
- Packet (message) headers identify recipients
- Packet routes can be tracked



Encryption does *not* hide routing information.

Who Needs Anonymity?

- Socially sensitive communicants:
  - Disease or crime victim chat rooms
- Law Enforcement:
  - Anonymous tips or crime reporting
  - Surveillance and honeypots (sting operations)
- Corporations:
  - Hiding collaborations of sensitive business units or partners
  - Hide procurement suppliers or patterns
- Political Dissidents
- Censorship resistant publishers
- Whistleblowers

Who Needs Anonymity?

- You:
  - Who are you sending email (who is sending you email)
  - What Web sites are you browsing
  - Where do you work, where are you from
  - What do you buy, what kind of physicians do you visit, what books do you read, ...

Who Needs Anonymity?

- Government

Government Needs Anonymity? Yes, for...

- Open source intelligence gathering
  - Hiding individual analysts is not enough
  - That a query was from a govt. source may be sensitive
- Defense in depth on open and *classified* networks
  - Networks with only cleared users (but a million of them)
- Dynamic and semitrusted international coalitions
  - Network can be shared without revealing existence or amount of communication between all parties
- Elections and Voting

Government Needs Anonymity? Yes, for...

- Networks partially under known hostile control
  - To attack comm. enemy must take down whole network
- Politically sensitive negotiations
- Road Warriors
- Protecting procurement patterns
- Homeland Security Information to/from municipalities, industry,...
- Anonymous tips (national security, congressional investigations, etc. In addition to law enforcement)

Existing Protections Can be Improved by Anonymity

- Virtual Hidden Networks
  - Traditional VPNs are not private
  - Anyone can see the network
  - Often adversary can see amount of communication
  - Onion Routing can provide anonymity to hide existence of private network and reduce countermeasure cost

Existing Protections Improved by Anonymity

- Location Hidden Survivable Services for
  - Homeland Security info to/from every town and industry
  - Censorship resistant publishers
  - Businesses with high value customers
- Hidden Server Properties
  - Servers accessible from anywhere
  - Resist attacks from authorized users
  - Resist Distributed DoS
  - Resist physical attack
  - Minimize redundancy, Reduce costs
  - Provide the above better than: firewalls, multiple redundant servers, physically hardened sites, IP filter, IP traceback

Who Needs Anonymity?

- And yes criminals

Who Needs Anonymity?

- And yes criminals

But they already have it.

We need to protect everyone else.

One Moral: For communication the real question is not,

How much privacy would you give up for security?

One Moral: For communication the real question is not,
How much privacy would you give up for security?

The question is,
How much security would you give up for <security?> ?

One Moral: For communication the real question is not,

How much privacy would you give up for security?

The question is,

How much security would you give up for <security?> ?

(and for anonymity there is no option to keep it to yourself)

Anonymity Loves Company

- You can't be anonymous by yourself
  - Can have confidentiality by yourself
- A network that protects only DoD network users won't hide that connections from that network are from Defense Dept.
- Need to share creates interesting incentive issues for network users and servers

Anonymous From Whom?
Adversary Model

- Recipient of your message
- Sender of your message

Need Channel and Data Anonymity

- Observer of network from outside
- Network Infrastructure (Insider)

Need Channel Anonymity

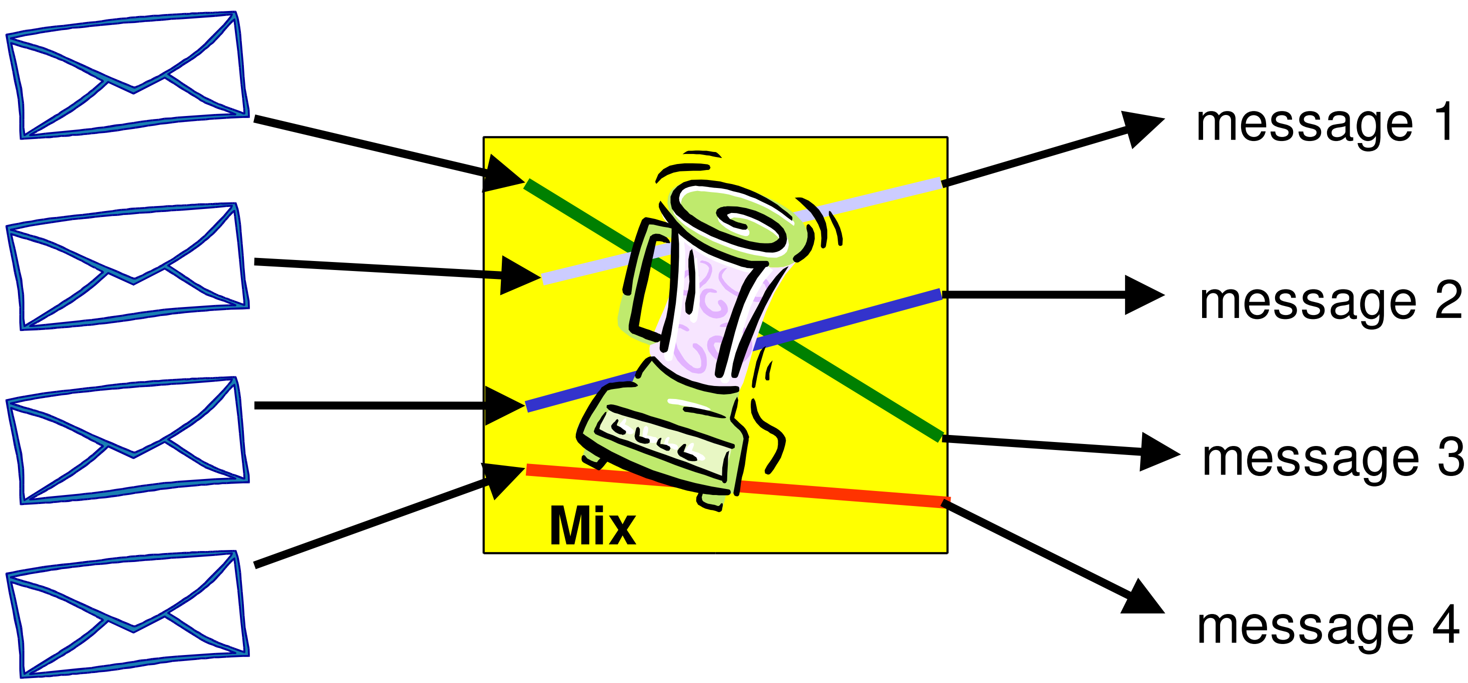
- Note: Anonymous authenticated communication makes perfect sense
- Communicant identification should be in the basic channel not of the channel

Focus of this work is anonymity of the communication pipe,
not what goes through it

How Do You Get Communication Anonymity?

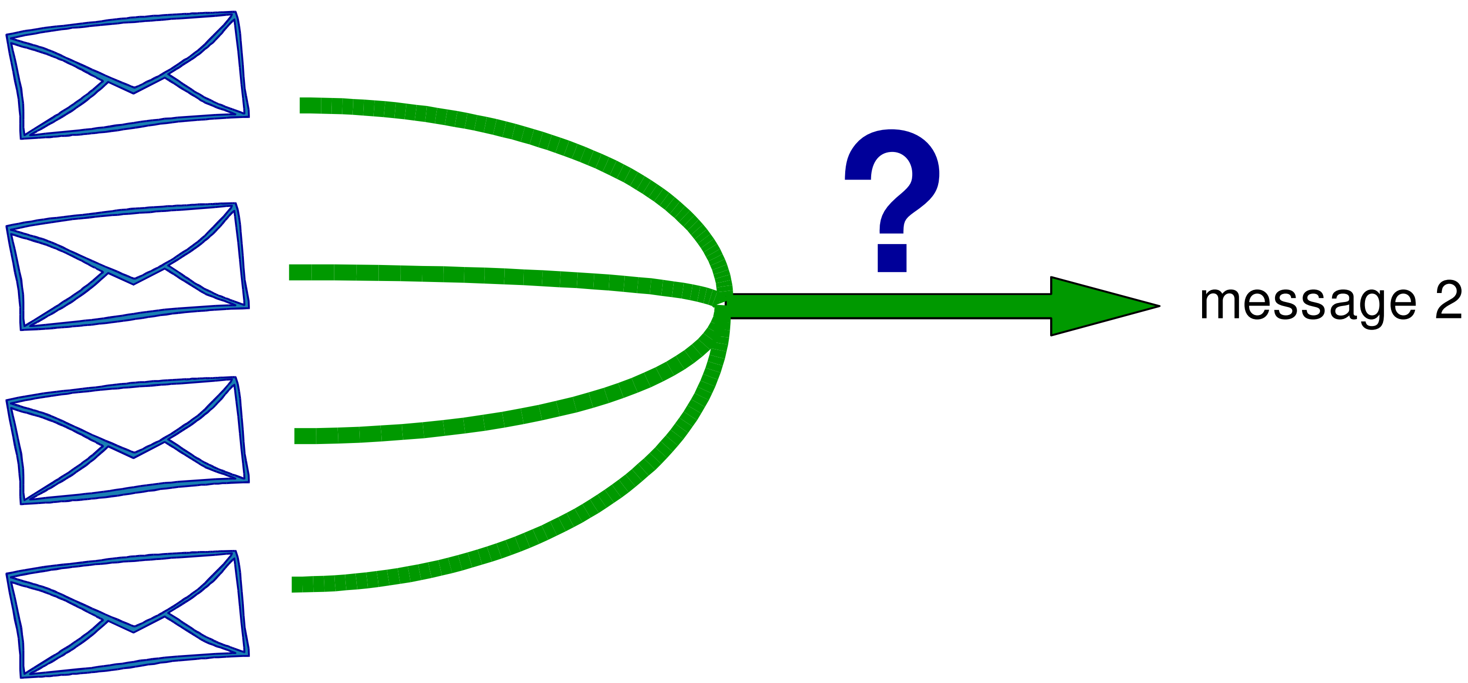
- Many technical approaches
- Overview of two extensively used approaches
  - Mixes
  - Proxies

What does a mix do?



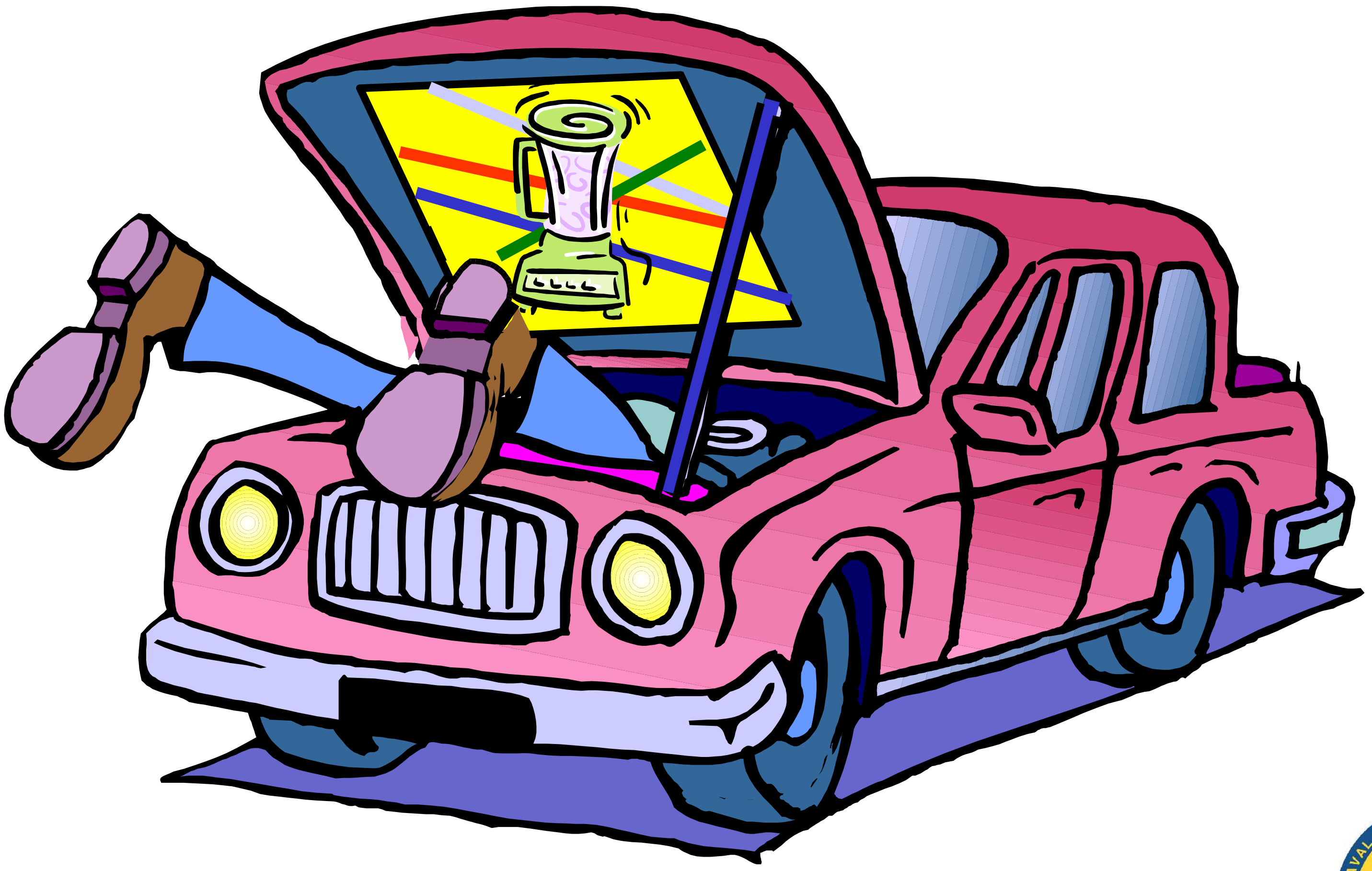
Randomly permutes and decrypts inputs

What does a mix do?

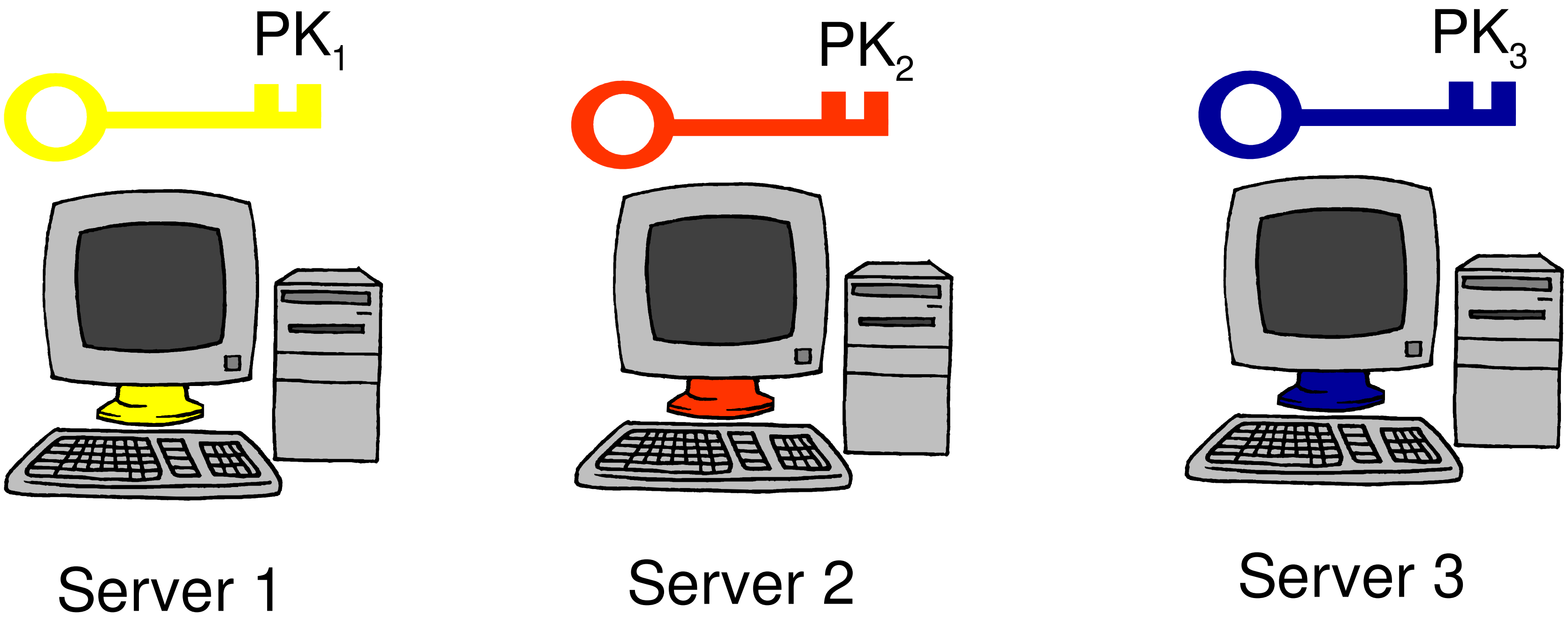


Key property: Adversary can't tell which ciphertext corresponds to a given message

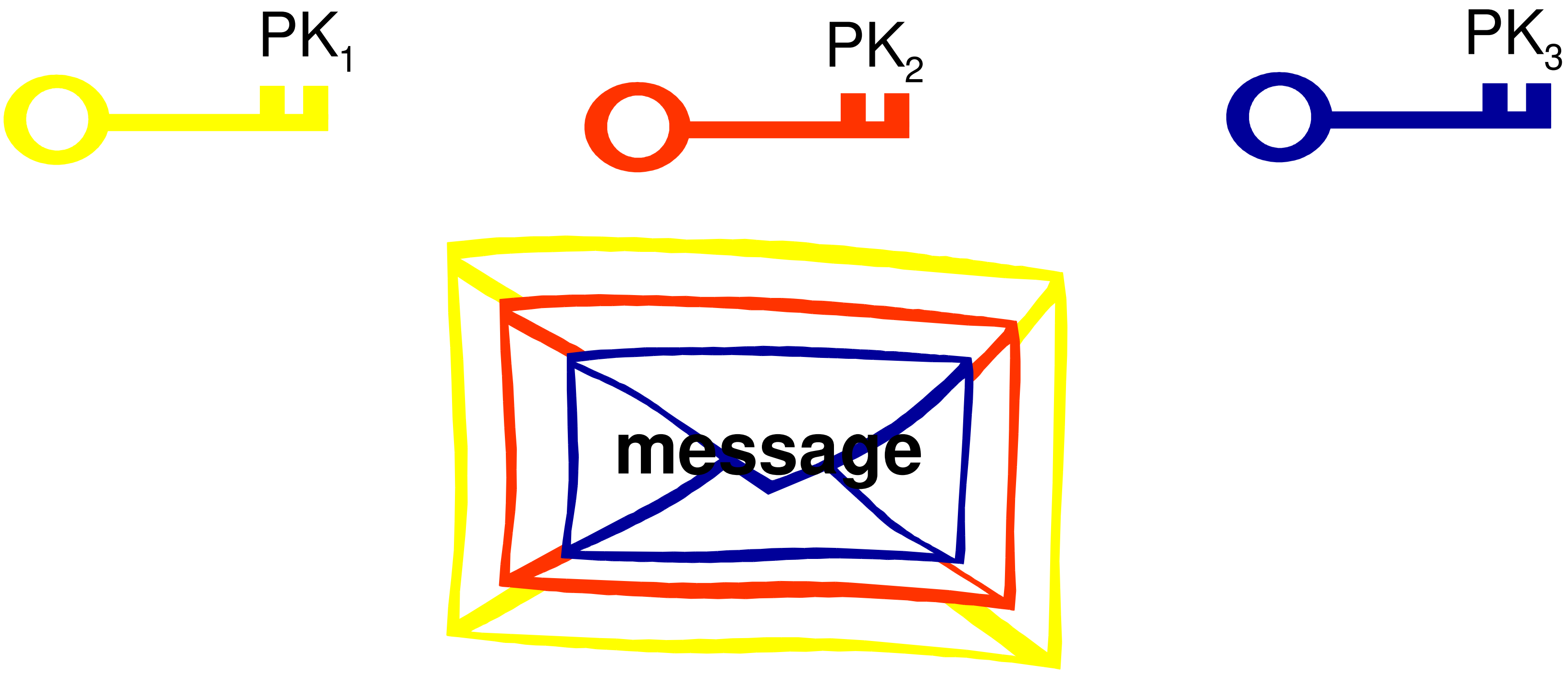
A look under the hood



Basic Mix (Chaum '81)



Encryption of Message



Ciphertext = $E_{PK1}[E_{PK2}[E_{PK3}[\text{message}]]]$

Basic Chaum-type Mix