SECURE COMMUNICATION:

ANONYMOUS COMMUNICATION

→ The internet is a public network

→ Routing info. is public — IP packet headers contain source & dest. of packets

→ Encryption does not hide identities — it hides payload, but not routing info.

∴ Routing info. can reveal what you're interested in on the Internet!
(What kinds of websites you go to) → Tracking for advertisements.

ANONYMITY

→ A user may use a service/resource w/o disclosing the user's identity

→ Can be achieved by hiding one's activities among others' similar activities:

1) Three-party Dining Cryptographers (3DC)

- 3 NSA cryptographers are having dinner. The waiter informs that the meal has been paid by someone: the NSA or one of the cryptographers. They want to know if it is NSA that paid, or one of them, w/o revealing identity

3DC PROTOCOL:

1) Every two cryptographers (Every pair) flip a coin that only they can see (heads = 1, tails = 0) (Generate random bit)

2) Each participant publicly announces the result as ff:
   - → Did NOT pay: the XOR of the two coin flips they observed
   - → Did pay: the negation of the XOR

3) If the XOR of the 3 announcements is
   - → 0: the NSA paid
   - → 1: one of them paid (but only the payer will know who)

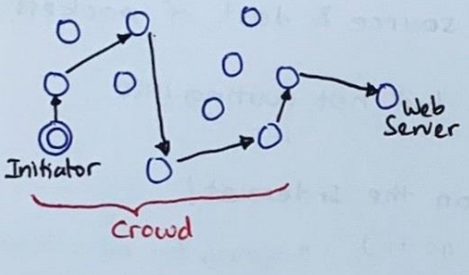
- 3DC protocol generalizes to any grp. size $n > 2$
- If a sender wants to anonymously broadcast a message m, the DC protocol is run for each bit of m (e.g. if m is 100 bits long, run protocol 100 times)

↳ IMPRACTICAL!!
- ↳ Requires pair-wise shared secret keys between the participants
- ↳ Requires large amt. of randomness
- ↳ Anyone can launch a DoS attack by not performing protocol properly

2) Crowds

→ IDEA — Randomly route the request through a crowd of users

→ A crowd is a grp. of m users; c out of m users may be corrupted

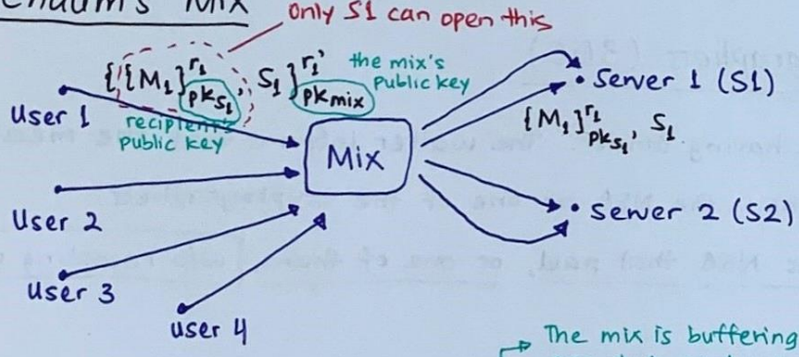


1) Initiator selects a forwarder from crowd and sends him his request
2) w/ probability $1-p_f$, a forwarder delivers the request directly to the server
   w/ probability p_f, he forwards the request to a randomly selected new forwarder from the crowd
3) Response from server follows same route in opp. direction

Crowd is not resistant against an attacker tht sees the whole network traffic.
(Global adversary)

SOLN

3) Chaum's Mix



The mix is buffering messages until it has enough to send out

↳ Message padding & buffering to avoid time correlation attacks

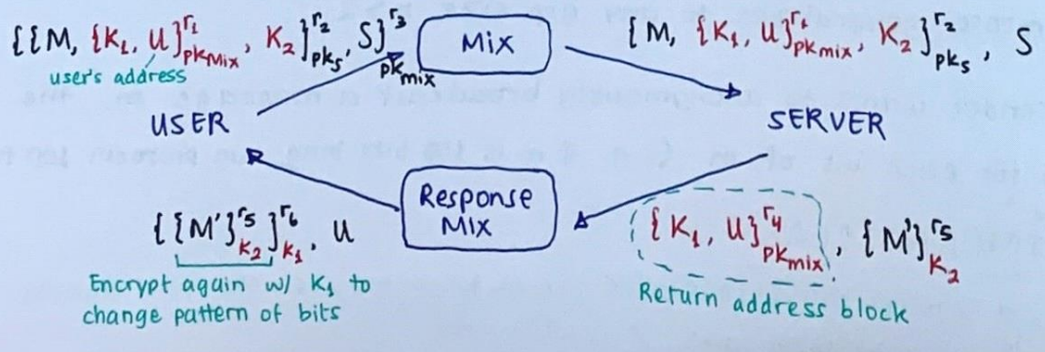
↳ Ensures messages are of same length; incoming & outgoing messages have same length

↳ The adversary can know the buffer size

↳ can send $n-1$ messages to a mix w/ capacity n allowing him to then link the sender of the n^{th} message w/ its recipient

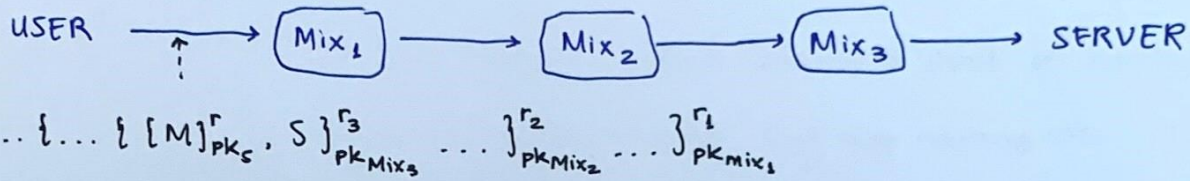
↳ Prevented by the mix through generating dummy messages

↳ What is needed now is a way for recipient to respond to sender while still keeping identity of sender secret from recipient



MIX CASCADE

→ Messages are sent through a sequence of mixes



$$\{ \ldots \{ \ldots \{ [M]^{r}_{pk_S}, S \}^{r_3}_{pk_{Mix_3}} \ldots \}^{r_2}_{pk_{Mix_2}} \ldots \}^{r_1}_{pk_{Mix_1}}$$

→ A single honest mix guarantees anonymity against an attacker provided it correctly applies:
- message padding
- buffering
- dummy messages

→ The more mix, the higher chance for an honest mix BUT add delay time for message to reach destination

LIMITATIONS

→ Asymmetric encryption
Dummy messages
Buffering
} NOT EFFICIENT !!