Anonymous Connections and Onion Routing

David Goldschlag, Michael Reed, and Paul Syverson

Center for High Assurance Computer Systems

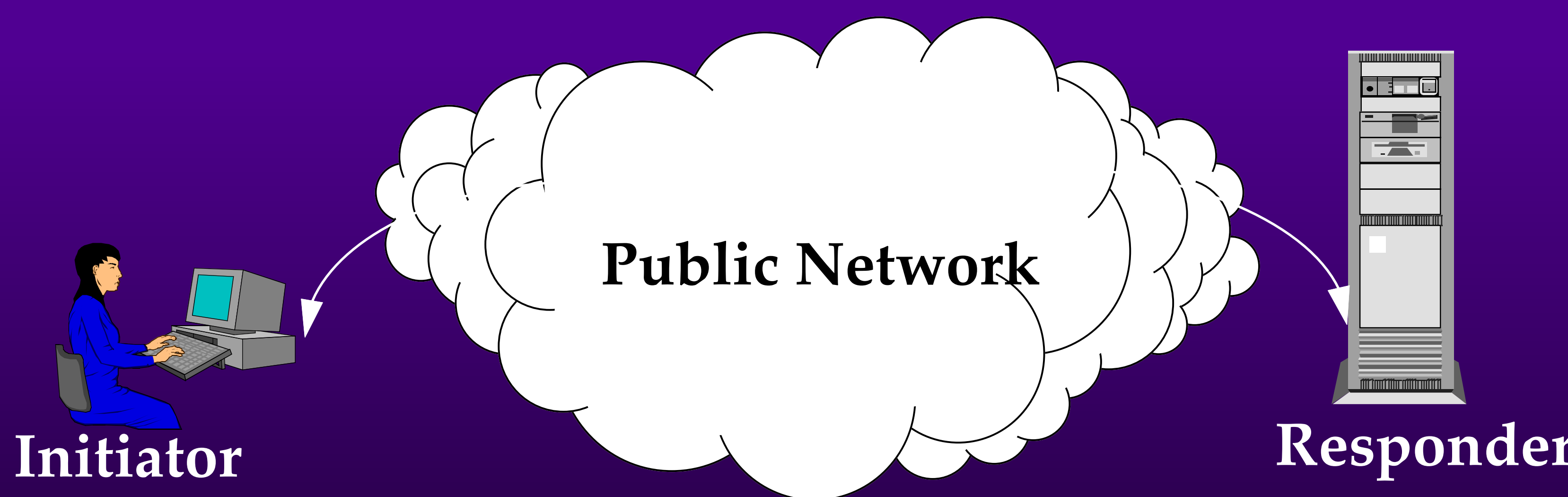
Naval Research Laboratory

Washington, D.C.

Who is Talking to Whom?

In a Public Network:

- Packet headers identify recipients
- Packet routes can be tracked



Encryption does *not* hide routing information.

Traffic Analysis Reveals Identities

***Who is talking to whom* may be confidential or private:**

- **Who is searching a public database?**
- **Which companies are collaborating?**
- **Who are you talking to via e-mail?**
- **Where do you shop on-line?**

Objective

Design an infrastructure that

- **Makes traffic analysis hard**
- **Separates identification from routing**
- **Is reusable across many applications**

Our goal is *anonymous connections*, not anonymous communication.

An infrastructure, *Onion Routing*, has been implemented.

Traffic Analysis

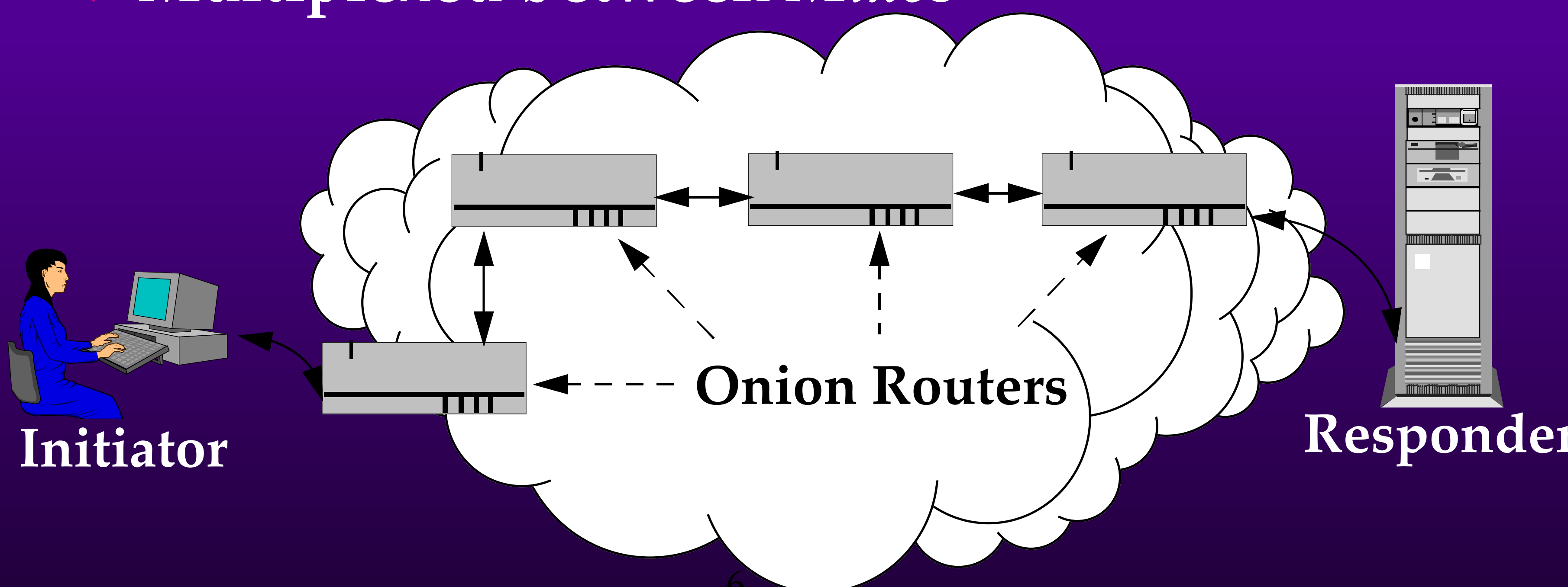
Focus on three components:

- **Hide routing headers**
- **Complicate statistical inferences**
- **Balance load**

Onion Routing: Network Infrastructure

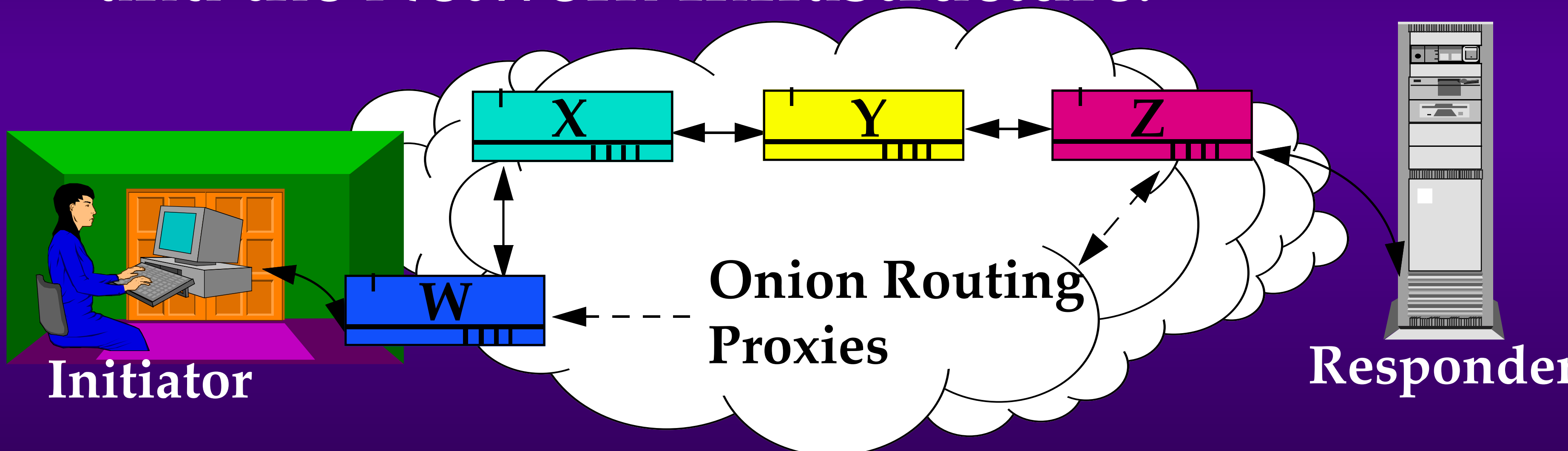
Anonymous connections are

- Routed through Chaum *Mixes*
- Multiplexed between *Mixes*



Onion Routing: Proxy Interface

Proxies interface between Applications and the Network Infrastructure.



The *Basic Configuration*: Sensitive sites control Onion Routing Proxies (which also function as intermediate Onion Routers).

Applications

Many applications can use Proxies:

- **Web browsing**
- **Remote login**
- **e-mail**
- **File transfer**

Threat Model: Active and Passive Attacks

- All traffic is visible
- All traffic can be modified
- Onion Routers may be compromised
- Compromised Onion Routers may cooperate
- Timing coincidences

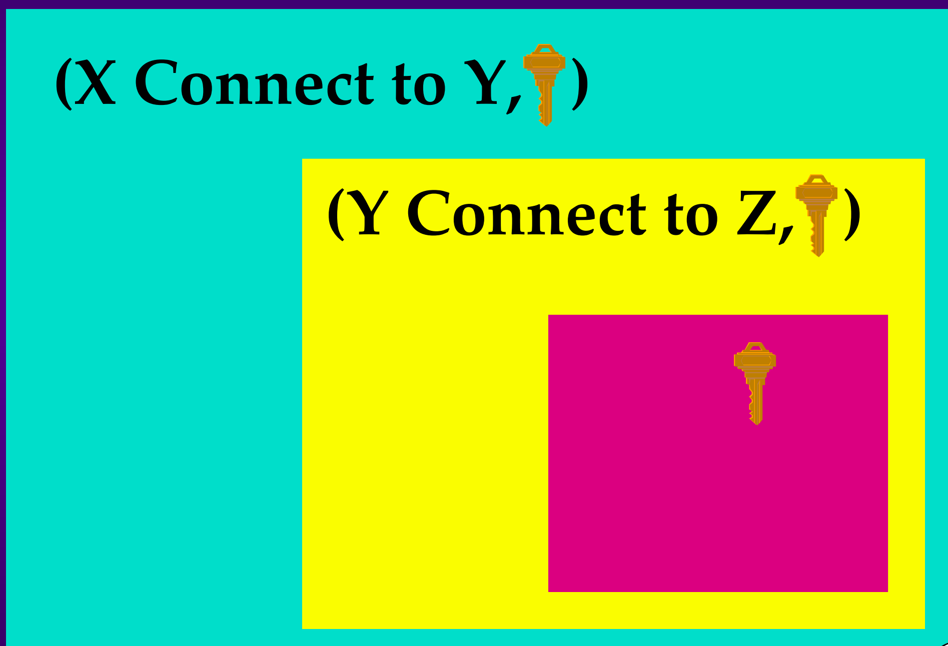
Using Onion Routing

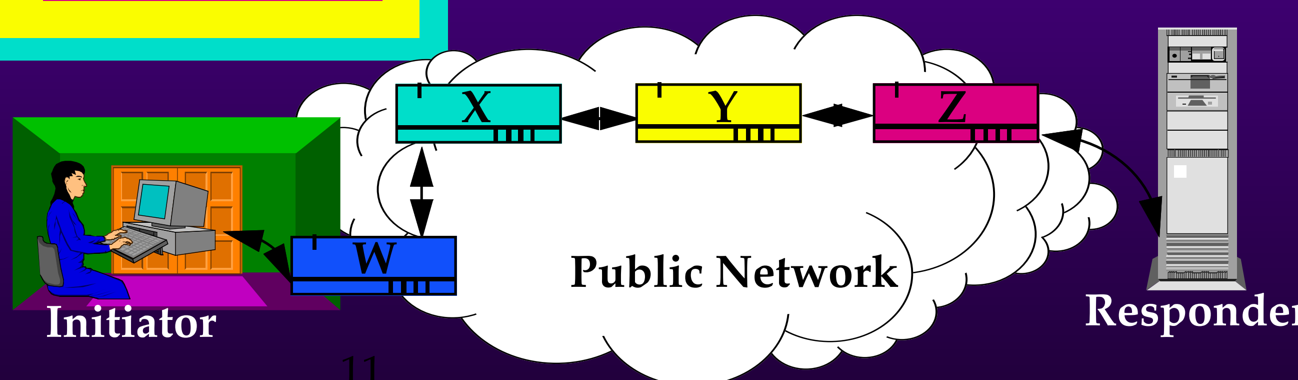
Four Steps:

- **Define the route**
- **Construct the anonymous connection**
- **Move data through the connection**
- **Destroy the anonymous connection**

Defining the Route

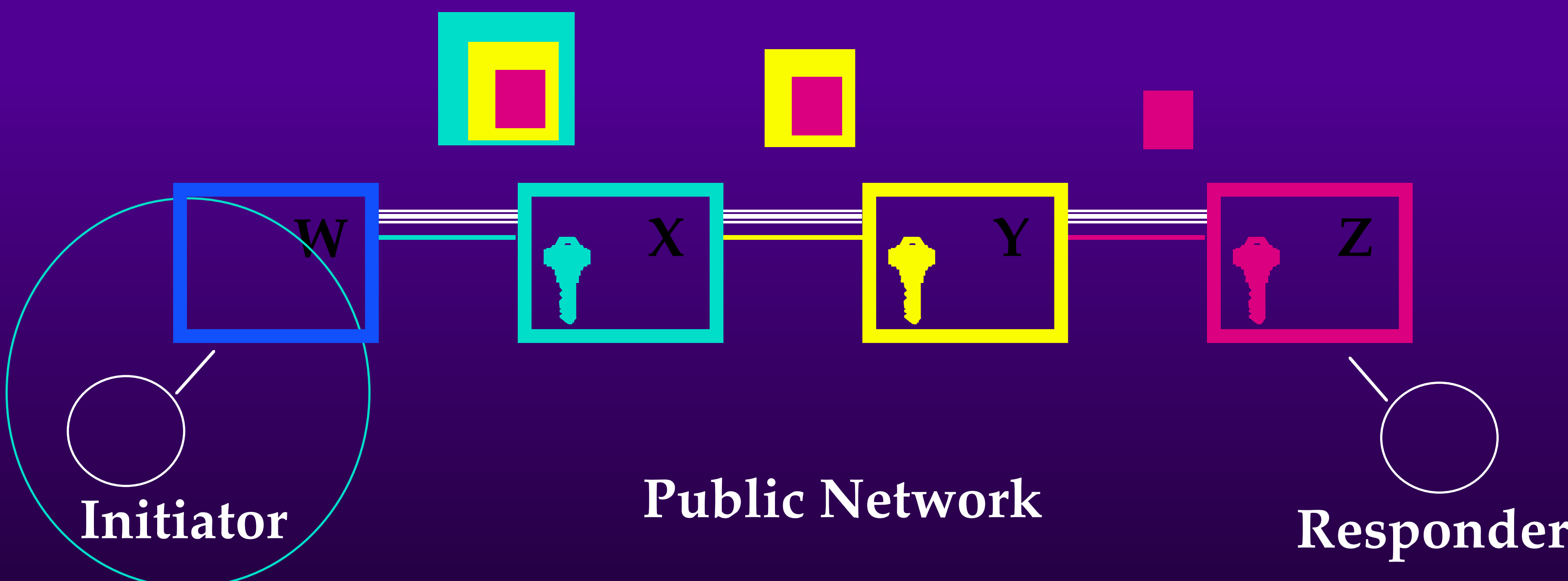
The Initiator's Proxy, W, makes an Onion:





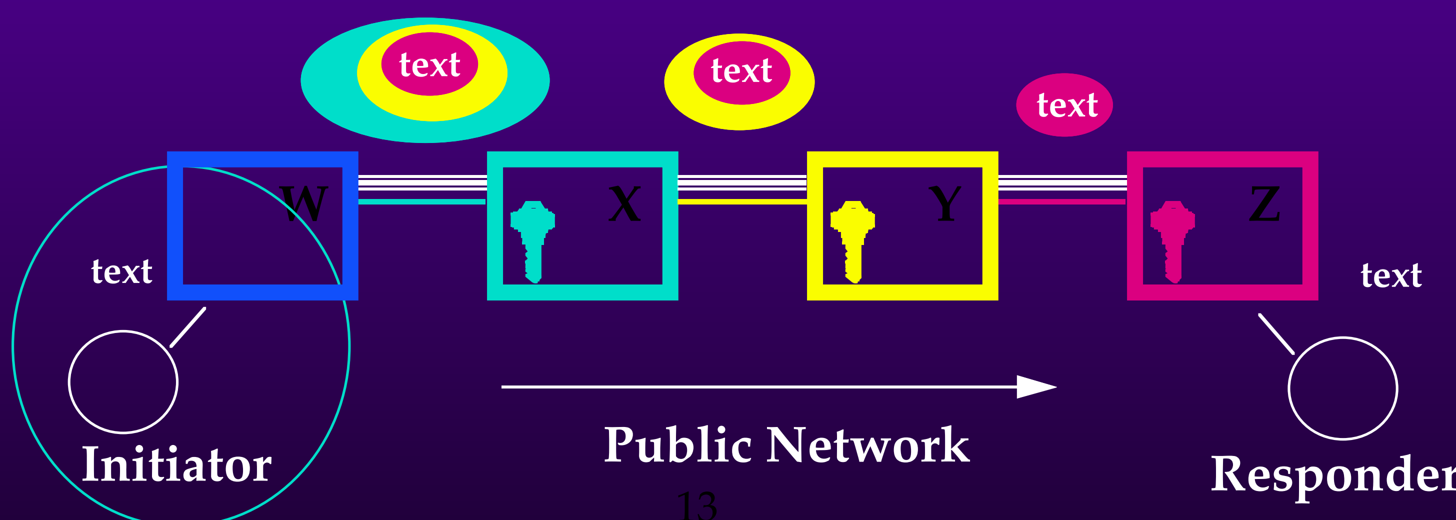
Constructing the Anonymous Connection

The Onion moves between Onion Routers.



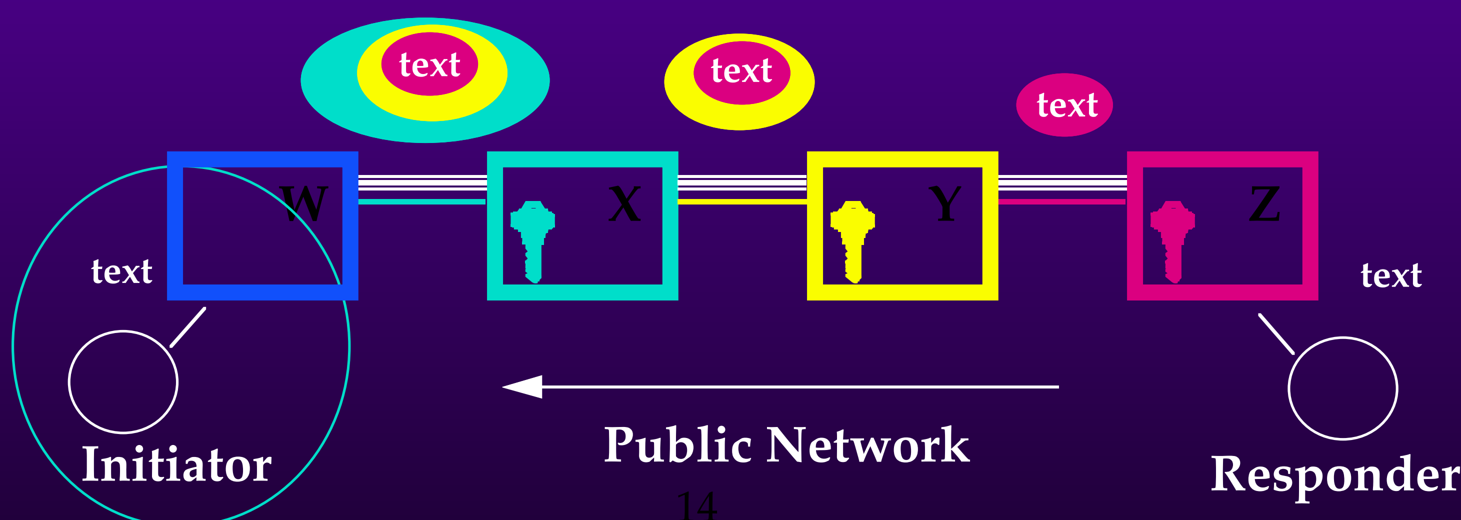
Moving Data Forward

- The Initiator's Onion Routing Proxy repeatedly crypts the data.
- Each Onion Router removes one layer of cryption.
- The Responder's Onion Routing Proxy forwards the plaintext to the Responder.



Moving Data Backward

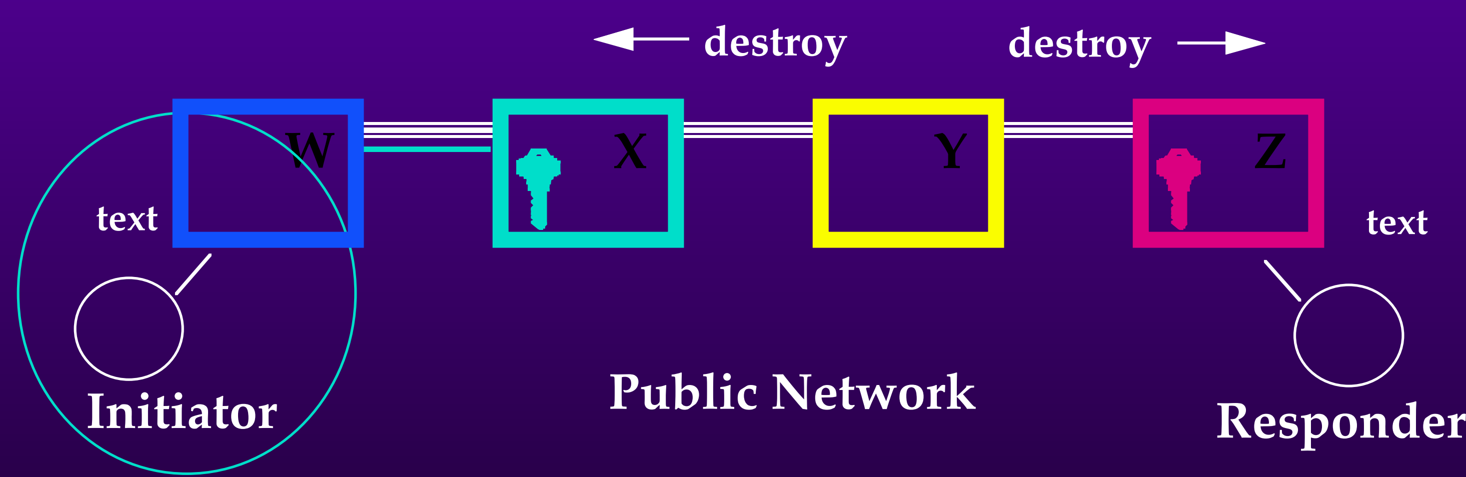
- This is just the reverse of sending data forward.
- Each Onion Router adds one layer of cryption.
- The Initiator's Onion Routing Proxy removes the layers of cryption and forwards the plaintext to the Initiator.



Destroying the Anonymous Connection

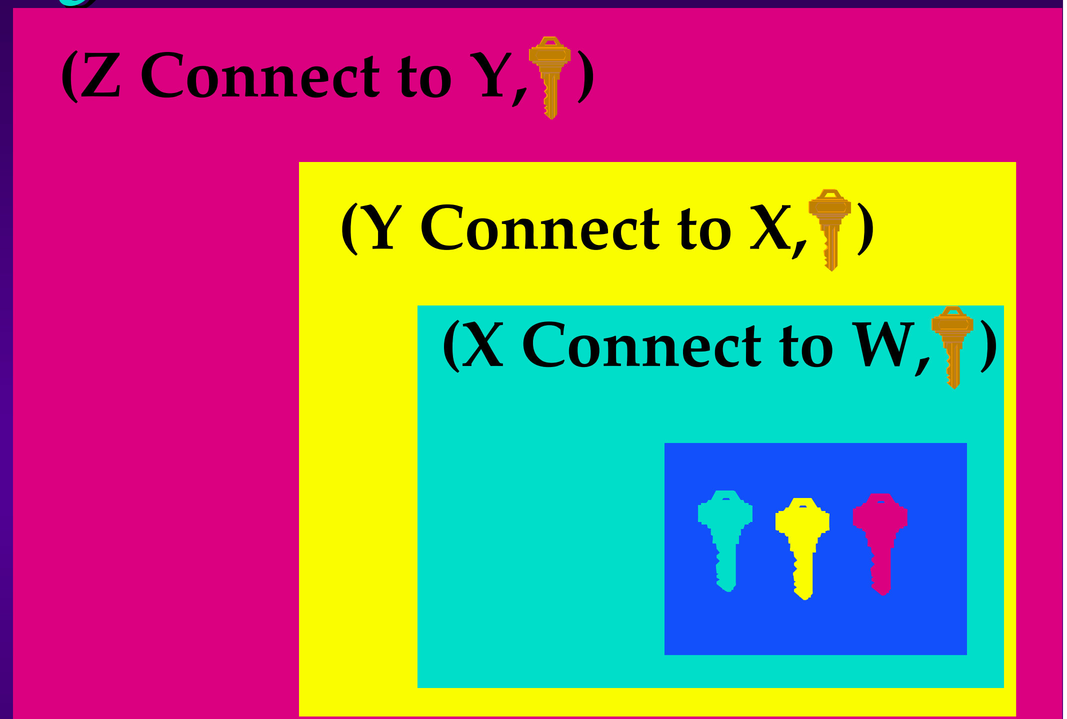
Destroy Messages

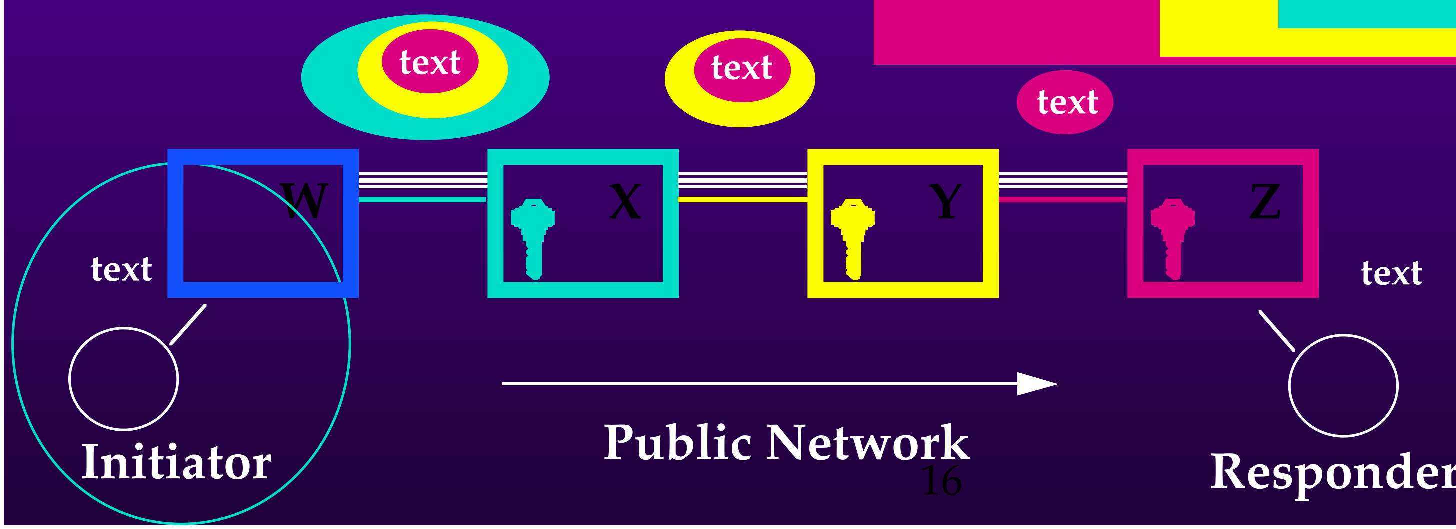
- **are forwarded along the connection**
- **cleaning up tables along the way**



Reply Onions

An Initiator's Onion Routing Proxy can create a Reply Onion that defines a route back to him.





Implementation

Working Onion Routing prototype.

Proxies for:

- **Web browsing (HTTP)**
- **Remote login (RLOGIN)**
- **e-mail (SMTP)**
- **File transfer (FTP)**

and anonymizing Web and mail proxies.

Performance

5 Onion Routers running on a single UltraSparc 2270.

Connection setup: 0.5 second cryptographic overhead.

(This cost can be amortized by using sockets for longer connections.)

Vulnerabilities

Timing Coincidences:

- **Do two parties often open new connections at the same time?**
- **This is not detectable in communication between two sensitive sites.**

Traffic Analysis: Load Balancing

- **Tradeoff between security and cost**
- **Is this feasible on the Internet?**

Onion Routing Network Configurations

The *Basic Configuration*

Hierarchical like the Internet

Customer--ISP Model

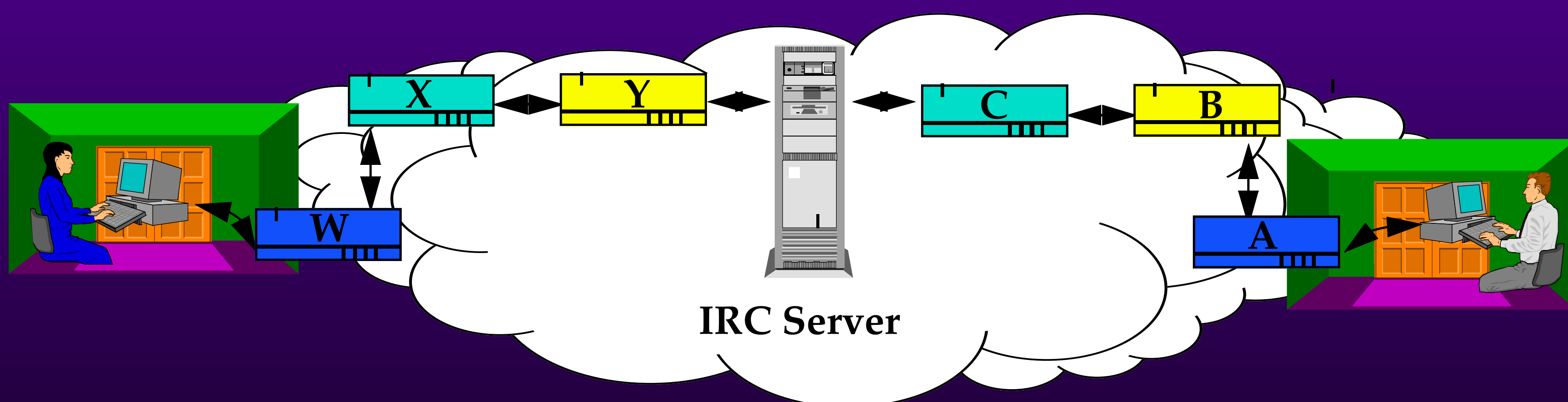
- **User makes onions on his PC**
- **PC routes through ISP's onion router**

Even the ISP cannot determine the PC's destination.

Other Applications

IRC: Two parties make anonymous connections to an IRC server, which mates the two connections.

Neither party has to trust the other.



Hide Location of Cellular Phones

To Make a Call:

- Phone makes anonymous connection to billing station through local base station.
- Phone identifies itself to billing station which completes the call.

To Call a Cellular Phone:

- Page the phone over a wide region.

Side Benefit:

- Very low standby power consumption.

Private Location Tracking

Active Badges

Competing Goals:

Track users's location.

But, keep location information private.

Home station tracks location:

- **Active badge contacts room sensor.**
- **Room sensor queries database for a reply onion over an anonymous connection.**
- **Sensor contacts home station using reply onion.**
- **Home station updates database over an anonymous connection.**

Discussion

- **Efficiency: Cryptographic overhead is no worse than link encryption between routers.**
- **Onion Routing Proxies must also be intermediate Onion Routers.**

Cryptographic Overhead

Along an (n+*1*)-Node route:

- **Data is encrypted n times**
- **Data is decrypted n times**

But, pre-crypting provides (for free):

- **Link encryption**
- **End to end encryption**
- **Data hiding: the same data looks *different* to each node**

Related Work

Chaum's Mixes

Babel: Mixes for e-mail

Anonymous ISDN: Mixes in a local ISDN switch

Conclusion

- **To be effective, *Onion Routing* must be widely used.**
- ***Onion Routing* supports a wide variety of unmodified services using *proxies*.**
- **Anonymity is placed at the application layer.**
- **The goal here is anonymous routing, not anonymity.**

References

http://www.itd.nrl.navy.mil/ITD/5540/projects/onion-routing

Who would like to run an Onion Router?