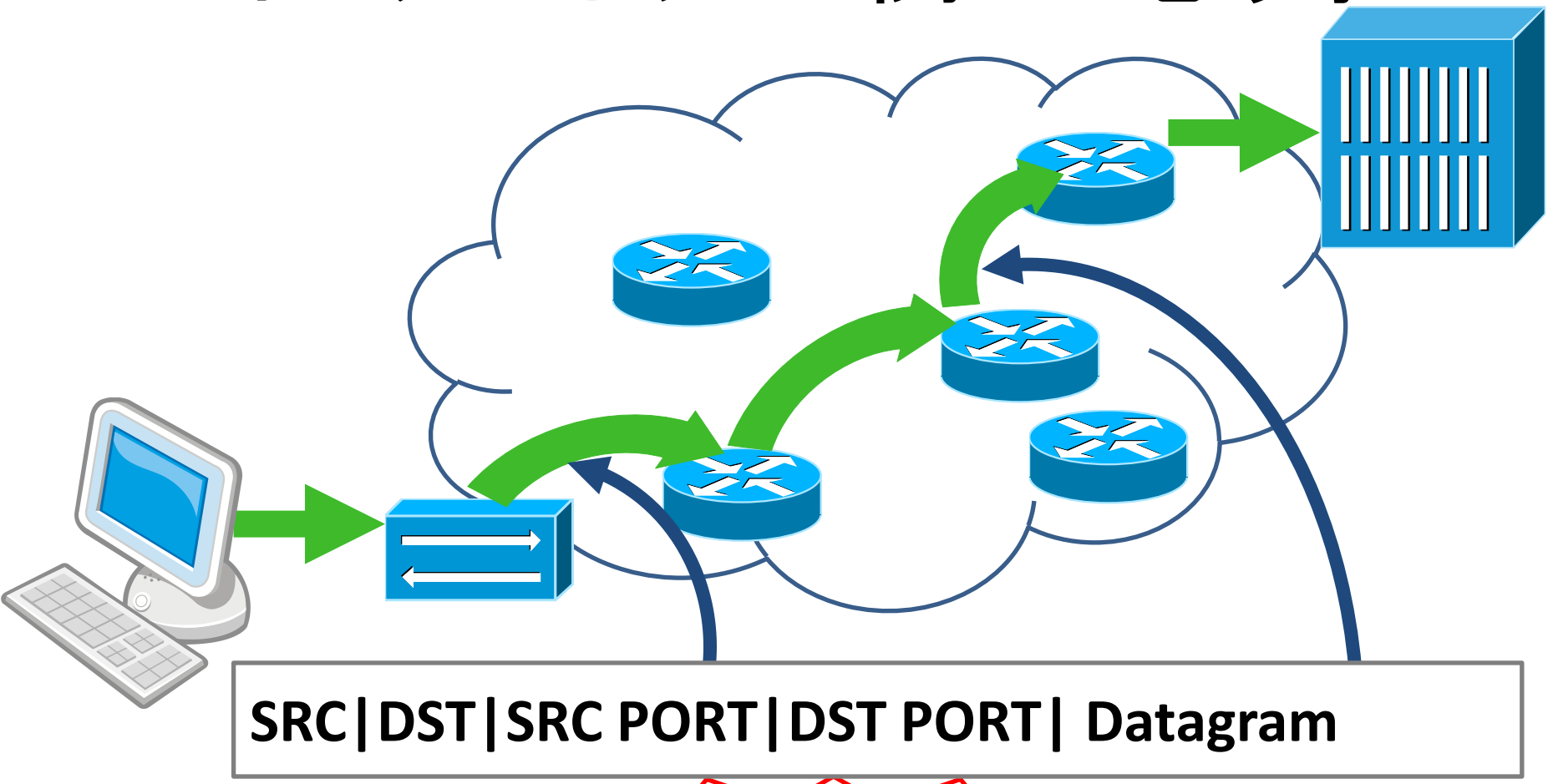
MAUI 20130624

bhangra

インターネットに関して想う事



SRC|DST|SRC PORT|DST PORT| Datagram

送信者も受信者も内容も
丸見えなのってイケてない

それなら匿名化システム

- 現在複数の匿名化システムが実用化されている

- システムはそれぞれファイル共有、検閲や弾圧に抵抗する為の匿名情報発信等のそれぞれの目的に基づいたデザインを持っている

匿名性の種類

- 送信者匿名性:
  - あるメッセージを発信した人物が受信者及び第三者からその発信した情報と紐付けられない事
- 受信者匿名性:
  - 特定のメッセージとそのメッセージの受信者が、他者から紐付けられない事
- 関係匿名性
  - 上記の2点より比較的に弱い匿名性となる。関係匿名性とは送信者と受信者が紐付けされない事

匿名性に貢献する技術

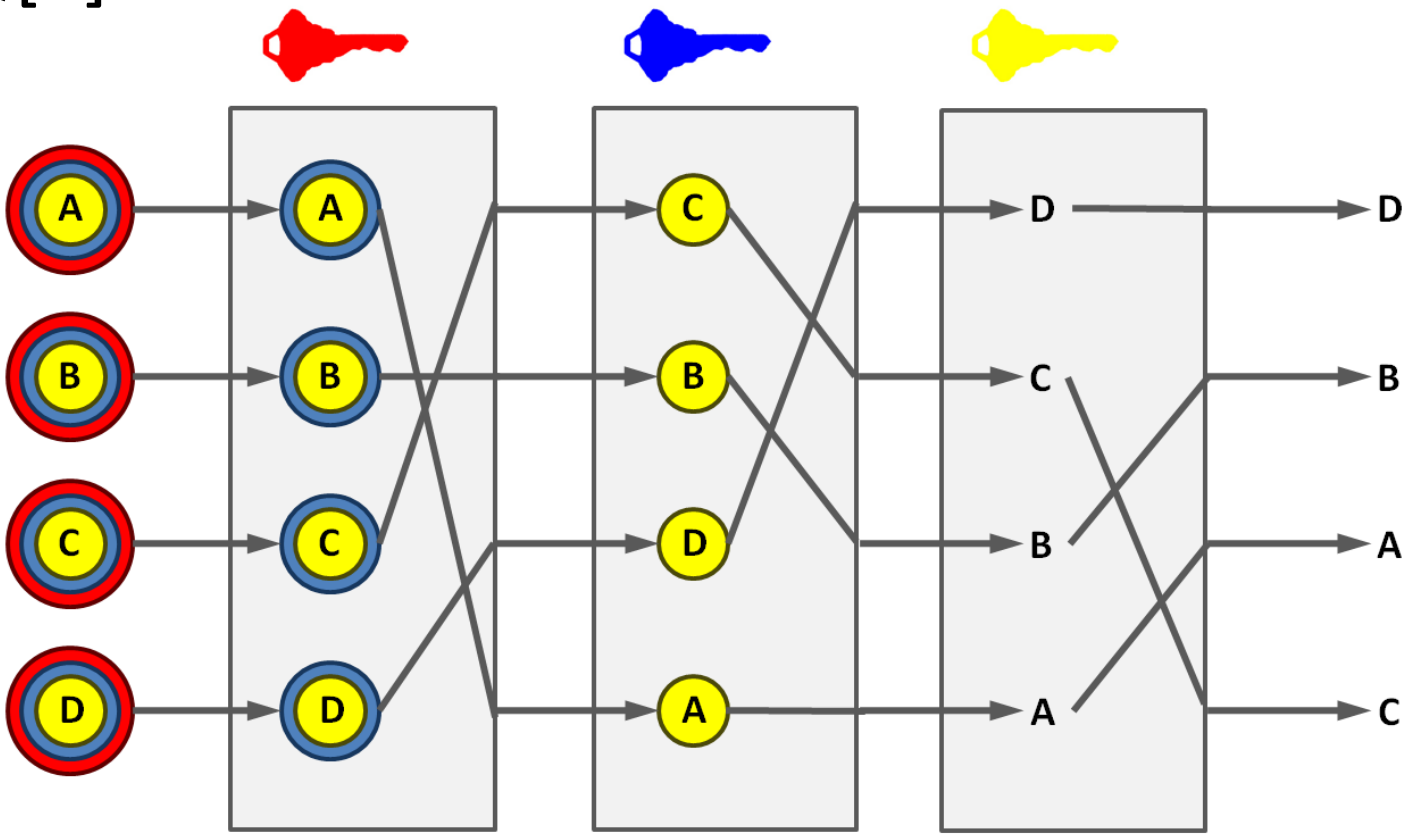
- 暗号化:
  - 通信内容の秘匿性の強化
- プロキシ:
  - 通信対象と利用者の間に入り、受信者を匿名化
- P2P:
  - ファイル等の情報の分散、ファイルの送信者等の秘匿化
- Onion Routing:
  - 分散オーバレイネットワークの構築、パケットの多重暗号化による送受信者及び通信内容の秘匿化

匿名化システムの評価軸

- 匿名性:
  - 送信者匿名性、受信者匿名性、関係匿名性等の強度
- 可用性:
  - その匿名化システムを介して利用可能なサービスや通信プロトコル
- 効率性:
  - 遅延、スループット

匿名化システムの始祖

- 1981年にChaum氏がmix-netのコンセプトを発表[1]



[1] Chaum, D. L. (1981). “Untraceable electronic mail, return addresses, and digital pseudonyms”. *Communications of the ACM* **24** (2): 84.
図はWikipediaの[Mix network]より転載(Primepq氏作)

Onion Routing

- 先述のChaum氏によるMix-netのデザインを基に米海軍調査研究所の出資により開発

- 複数のMix間をメッセージが動的にルーティングする事により送受信者とメッセージ内容の匿名性を強化

- 複数のメッセージを同梱する事により解析を困難にする Garlic Routingと称される技術もある: I2P、Perfect Dark等が例としてあげられる

実用化例: Tor

- Onion Routingに以下の実装を追加
  - Perfect Forward Secrecy
  - 輻輳制御
  - ディレクトリサーバ
  - Exit Policyを設定可能に
  - 実用的な秘匿サービス
- P2Pではない

Torの問題

- パフォーマンス
- セキュリティ
  - 2007年にEgerstad氏がExitルータを設置し、日本を含む各国の大使館や人権団体の通信の傍受に成功

今後