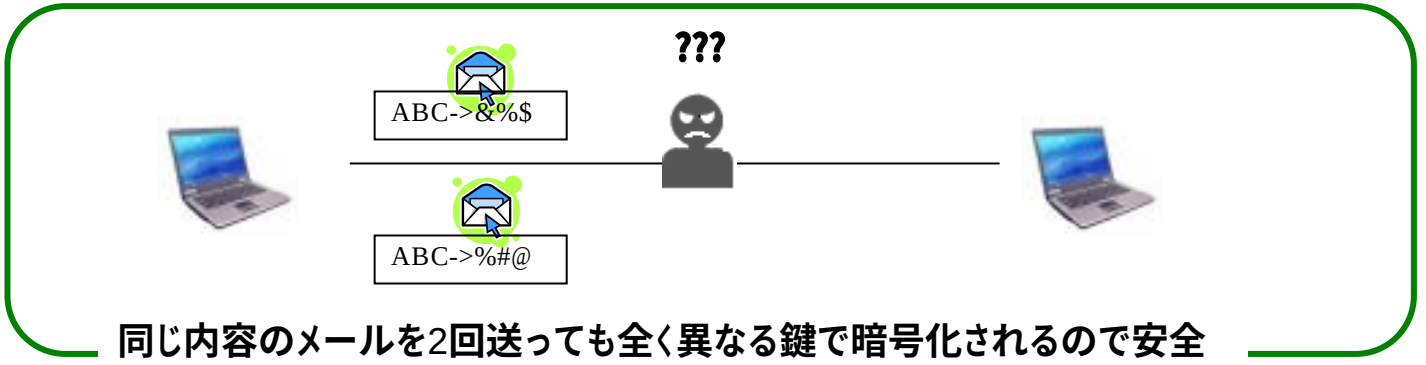
BitTorrent型分散システムと使い捨てパッドを用いた通信システムの開発

石井　充

使い捨てパッド：　絶対に解読できないことが数学的に証明されている暗号

↓

既存の暗号と異なり100%安全な暗号



同じ内容のメールを2回送っても全く異なる鍵で暗号化されるので安全

既存の問題点

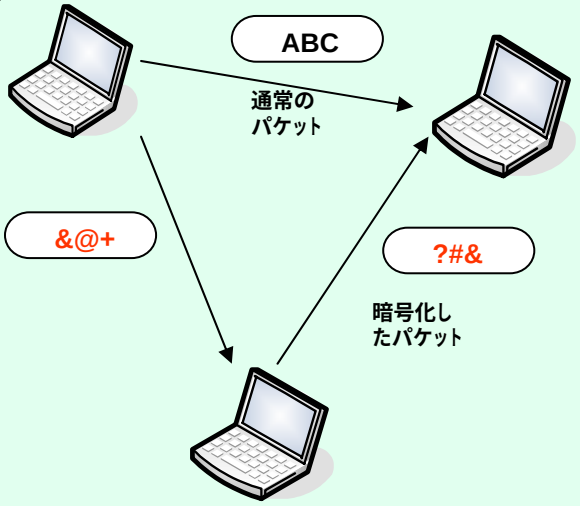
- 使い捨てパッドでは鍵の長さが平文データと同じ
- 鍵を安全に配信する方法がない

→

解決方法

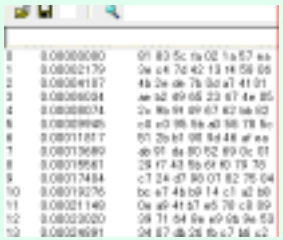
- BitTorrent方式の分散システムを利用
- Diffie-Hellmanを用いて鍵を共有

社内LANの場合

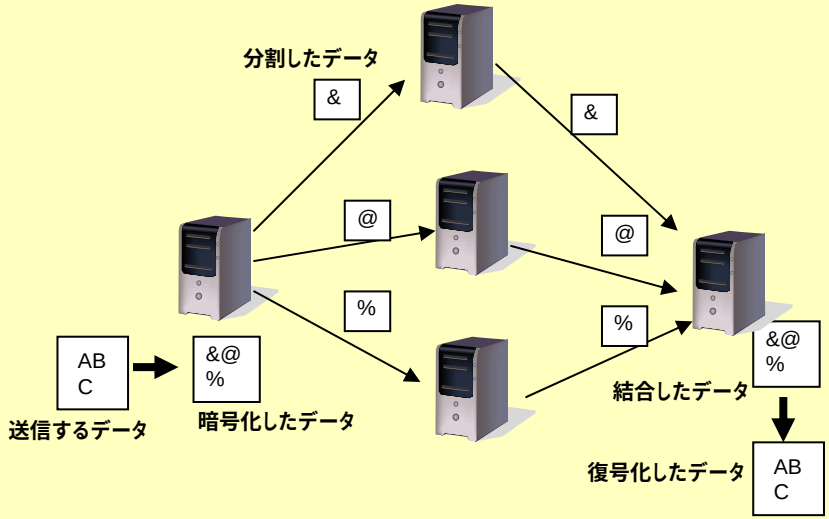


パケット単位で暗号化

- Diffie-Hellmanによる鍵共有
- TCP/IPのヘッダーまで暗号化
- 暗号化される対象PCを自由に設定可能
- ドライバーをインストールするだけで、特別なソフトは必要なし



社外ネットの場合



暗号化して分割配信

→ 使い捨てパスワードは毎回変わるので盗まれても安全

- 分割して送信･障害対応可能
- 異なる経路で配信して安全を確保
- ハッシュ値を確認し、改ざん対策

両手法を用いて、全通信で使い捨てパッドによる暗号化が可能