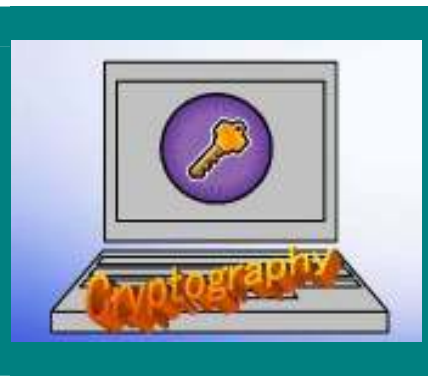
コンピュータとインターネット時代に
数値シュミレーションと暗号技術で
未来を拓く

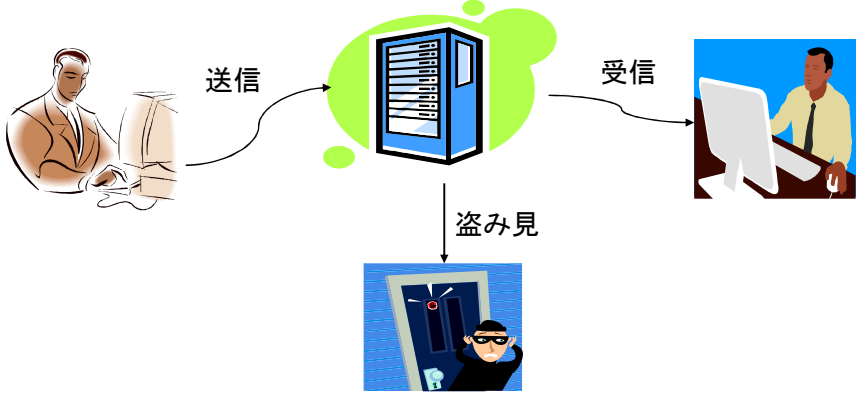


コンピュータ応用学科 **数値シミュレーション研究室**

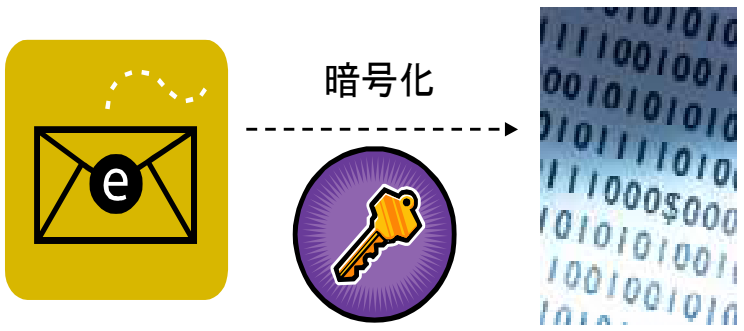
研究内容 電子社会の安全を保つ暗号技術

通信における暗号の必要性

完全な盗聴防止は不可能

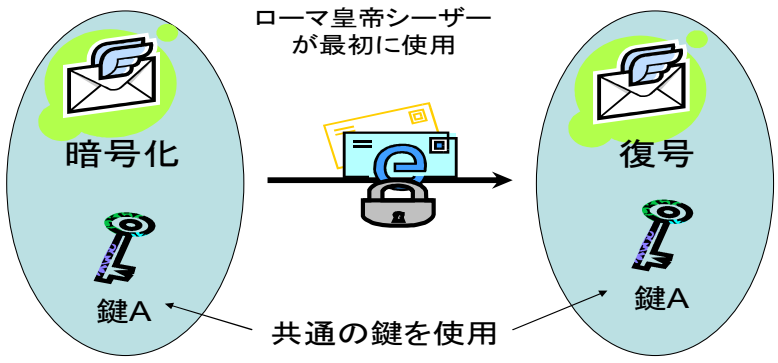


暗号化して安全に通信



現在使用されている暗号

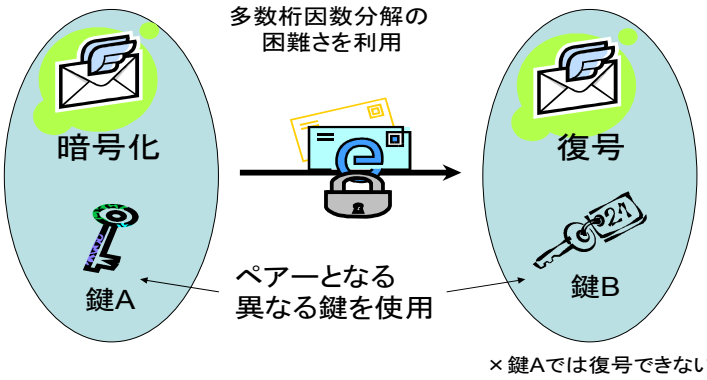
共通鍵暗号



鍵を送る必要がある

両方を使用

公開鍵暗号(RSA暗号)



暗号化に時間がかかる

ハイブリッド暗号

インターネットで使用している暗号を調べる

http： 暗号を使用しない通信

https: 暗号を使用した通信 → web ページを右クリック→プロパティ

→ 接続：SSL 3.0、RC4/128 ビット暗号(高)
RSA 1024 ビット交換

SSL: ハイブリッド暗号、RC4 ：共通鍵暗号、RSA ：公開鍵暗号