応用 B

無線秘密鍵共有

Wireless Secret Key Agreement System

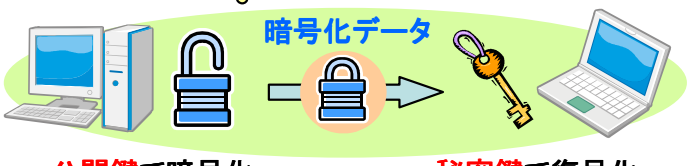
近年無線による通信が増加！
↓
電波は誰でも受信できる
↓
情報を盗まれるかもしれない

→ 情報を暗号化しよう！

暗号化には鍵が必要！

暗号化方式

公開鍵方式

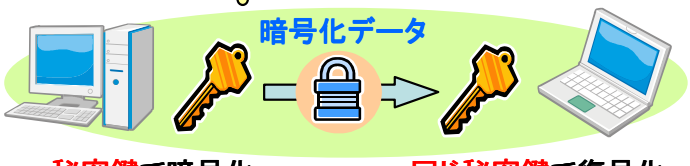


公開鍵で暗号化　　秘密鍵で復号化

利点：鍵を共有する必要がない

欠点：計算機の性能向上で解読されてしまう

秘密鍵方式



秘密鍵で暗号化　　同じ秘密鍵で復号化

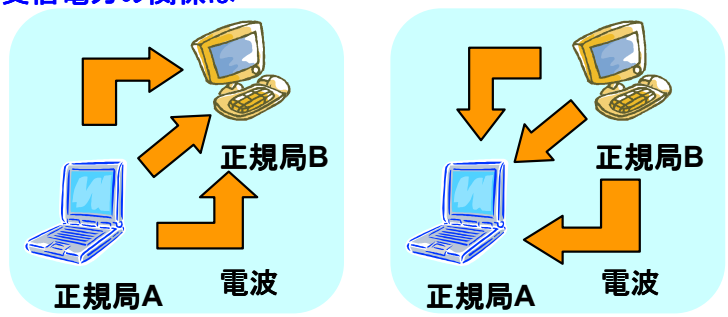
利点：計算機の性能に関係なく安全

欠点：鍵の安全な共有が必要

秘密鍵を安全に共有したい！

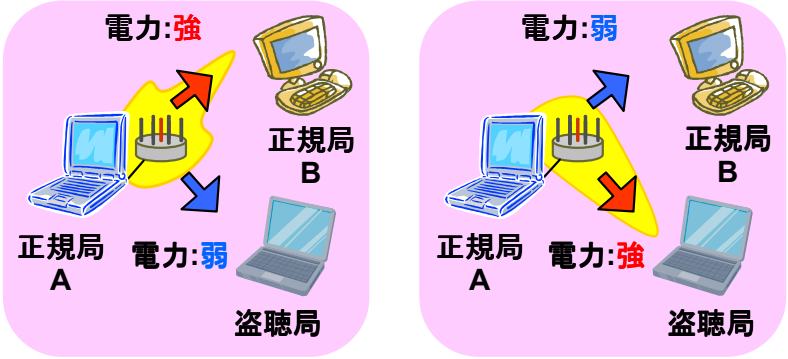
そこで新提案！可変指向性アンテナを用いた秘密鍵共有方式

受信電力の関係は・・・



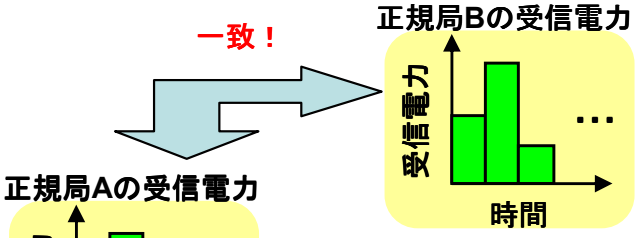
伝搬経路が同じなのでAとBは同じ受信電力

指向性を時間的に変化させると・・・

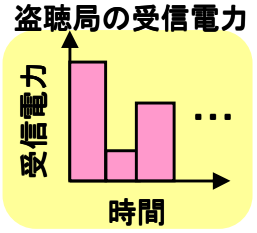


時間的に受信電力が変化

一致！



異なる



受信電力を鍵にする！

受信した電力から鍵を推測できない！

研究課題

- 雑音の影響で鍵が一致しない
- 盗聴に対する対策を考える
- この方式は本当に使えるのか

→

- 正規局間における鍵の一致率向上
- 正規局・盗聴局との一致率抑制
- 実験による検証