Comp Security and Psuedo One Time Pads

Do PRGs exist?

1. We don't know

Do PRGs exist?

1. We don't know . . . Would imply P $\neq$ NP
2. We will *assume* certain algorithms are PRGs
3. Can *construct* PRGs from weaker assumptions (Chap 7)

Using Pseudo one-time pad

- Let G be a deterministic algorithm, with $|G(k)| = p(|k|)$
- $Gen(1^n)$: output uniform n-bit key k
  - Security parameter $n \Rightarrow$ message space $\{0,1\}^{p(n)}$
- $Enc_k(m)$: output $G(k) \oplus m$
- $Dec_k(n)$: output $G(k) \oplus c$
- correctness is obvious

Security of pseudo-OTP?

Theorem: Pseudo-OTP is comp secure.

Proof Sketch: Can show that if not comp secure then G is not PRG. We omit details.

Stepping back

- *Proof* that the pseudo OTP is secure . . .
- . . . with some caveats
  - Assuming G is a pseudorandom generator
  - Relative to our definition
- The *Only* way the scheme can be broken is:
  - If a weakness is found in G
  - If the definition isn't sufficiently strong . . .

Have we gained anything?

- YES: the pseudo-OTP has a key shorter than the message
  - n bits vs. p(n) bits
- The fact that the parties *internally* generate a p(n)-bit string to encrypt/decrypt is irrelevant
  - The *key* is what the parties share *in advance*
  - In real-world implementation, could avoid storing entire p(n)-bit temporary value

Recall . . .

- Perfect secrecy has two limitations/drawbacks
  - Key as long as the message
  - Key can only be used once
- We have seen how to circumvent the first
- the pseudo OTP still has the second limitation (for the same reason as the OTP)
- How can we circumvent the second?

Our Goal

With psuedo OTP can securely send one n-bit message. Yeah!

Our Goal

With psuedo OTP can securely send one n-bit message. Yeah!

If use same key then cannot send another n-bit message. Boo!

Our Goal

With psuedo OTP can securely send one n-bit message. Yeah!

If use same key then cannot send another n-bit message. Boo!

We want to send multiple message with same key.

But first . . .

- Develop an appropriate security definition
- Recall that security definitions have two parts
  - Security goal
  - Threat model
- We will keep the security goal the same, but strengthen the threat model