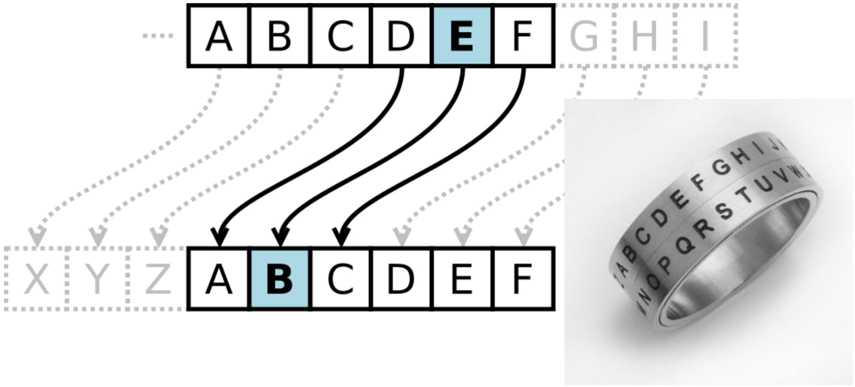
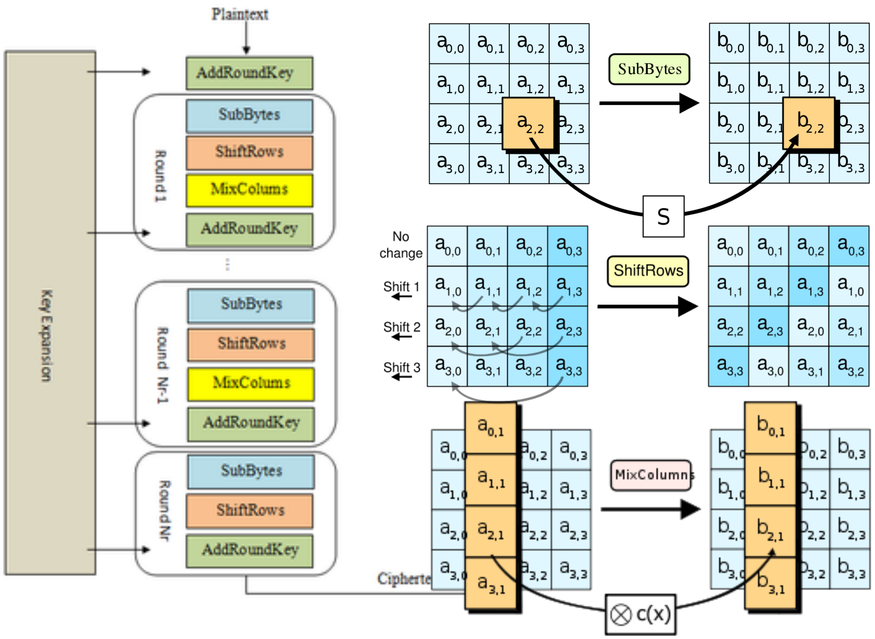
Lecture 9: Protocols

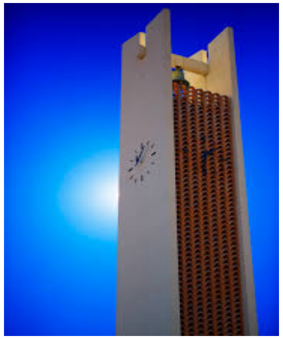
CS 181S

October 3, 2018

Crypto Thus Far…

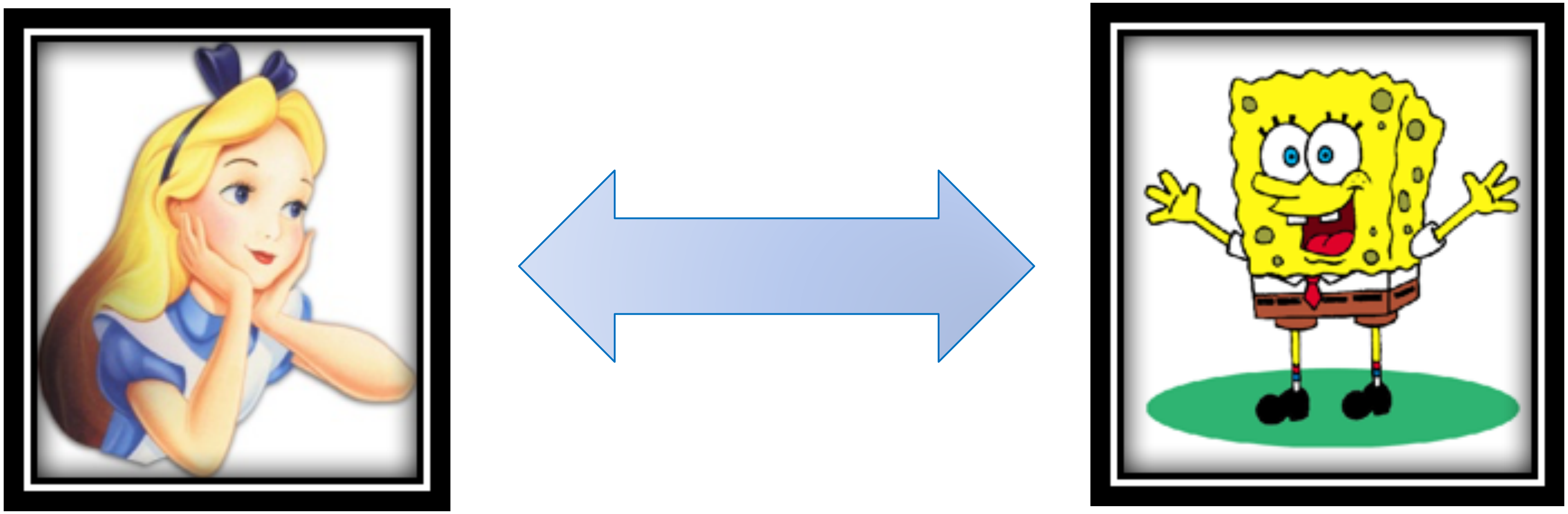






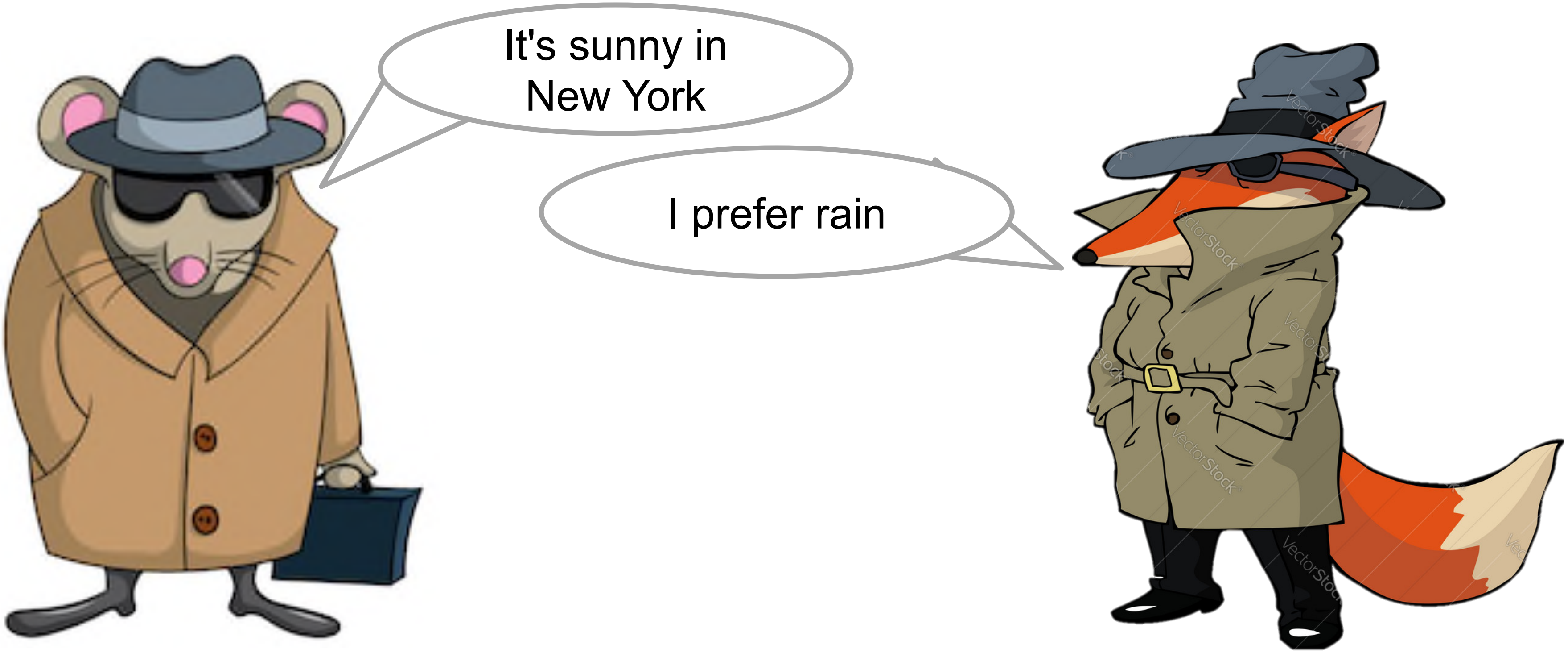
Sign
Signature

Monday: Secure Channels



Today: Authentication Protocols

- An **authentication protocol** allows a principal receiving a message to determine which principal sent that message



Threat Model

- Dolev-Yao attacker
  - controls the network, can read, modify, create packets

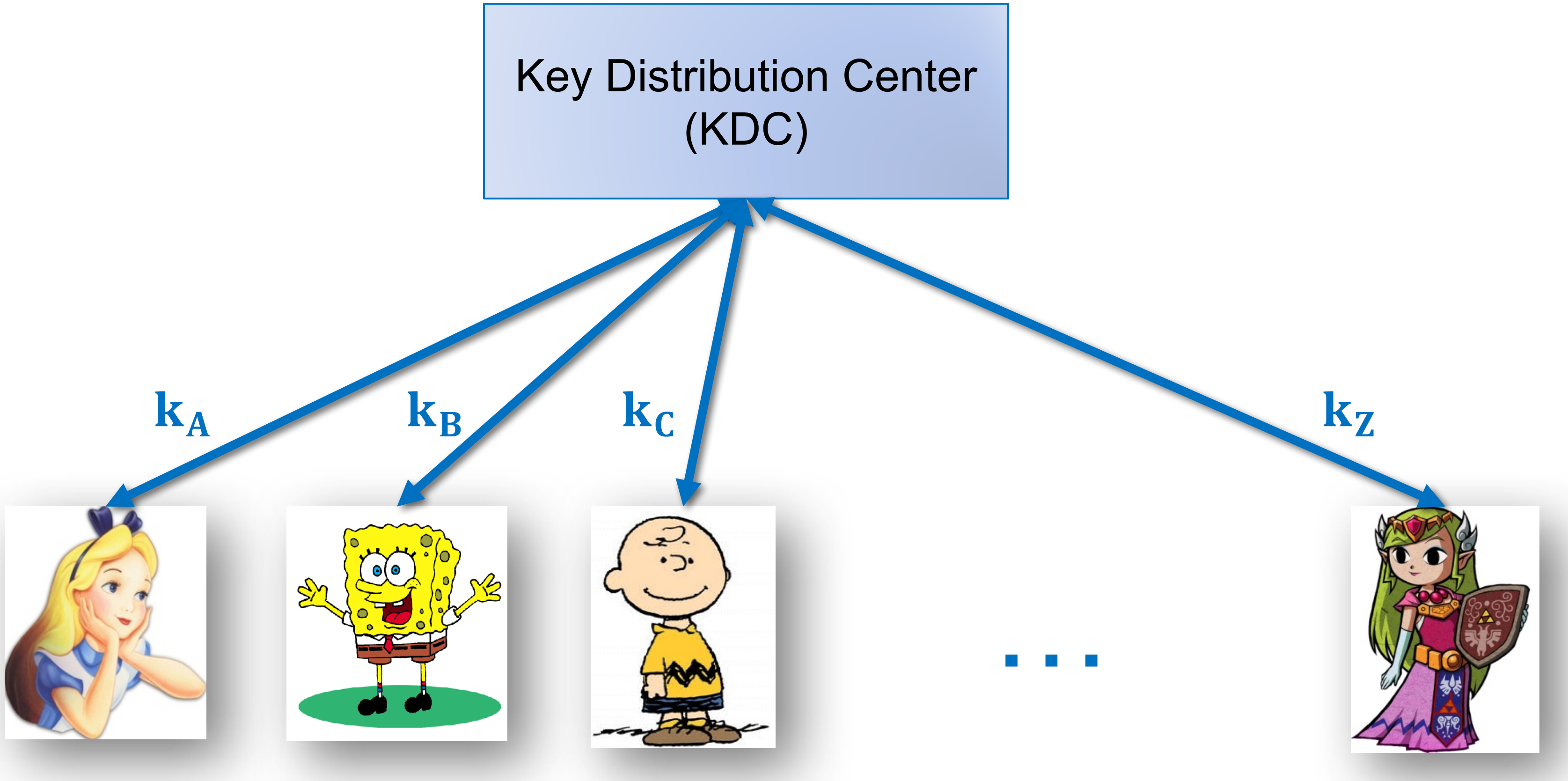
- A **replay attack** occurs when an adversary repeats fragments of a previous protocol run
- A **reflection attack** occurs when an adversary sends messages from an ongoing protocol back to the originator
- A **man-in-the-middle attack** occurs when an adversary secretly relays (and potentially changes) communications between two principals who believe they are communicating directly with eachother

Authentication with Symmetric Keys

- Assumption: Alice and Bob have a shared key k_AB

1. B: r <- {0,1}^n
2. B -> A: B, r
3. A -> B: Enc(A, r; k_AB)
4. B: check whether Dec(m3; k_AB) = (A, r)

Key Distribution Protocols



Key Distribution Center (KDC)

k_A

k_B

k_C

. . .

k_Z

Needham-Schroeder

1. A -> KDC: A, B, r
2. KDC -> A: Enc(A, B, r, k_AB; k_B)
3. A->B: A, B, Enc(A, B, k_AB; k_B)
4. B->A: Enc(r'; k_AB)
5. A->B: Enc(r'+1; k_AB)

Otway-Rees

1. A->B: n, A, B, Enc(r1, n, A, B; k_A)
2. B->KDC: n, A, B, Enc(r1, n, A, B; k_A)
3. KDC->B: n, Enc(r1, k_AB; k_A), Enc(r2, k_AB; k_B)
4. B->A: n, Enc(r1, k_AB; k_A)