Security Protocols

Unlock Scheme 0

I’m a key!

Good enough for me.
TOGGLE LOCK

Unlock Scheme 1

I’m the key for car 14165

That’s me!
TOGGLE LOCK

Unlock Scheme 2

I'm the key for car 14165
and I want you to UNLOCK

That's me!
UNLOCK

Unlock Scheme 2

16-bit password = 2^16 possibilities = average 2^15 tries ~= 1 hour

Nonces

“Number used **once”**

I’m the key for car 14165
and I want you to UNLOCK
Also: “24”

That’s me! Not seen
that nonce before, either.
UNLOCK

Nonce Scheme 1

```
if nonce == last_nonce:
  DENY
else:
  ACCEPT
  last_nonce = nonce
```

Nonce Scheme 2

```
known_nonces = circ_buff(10)
if nonce in known_nonces:
  DENY
else:
  ACCEPT
  known_nonces.add(nonce)
```

Valet attack

Park my car, Brutus

<valid token>

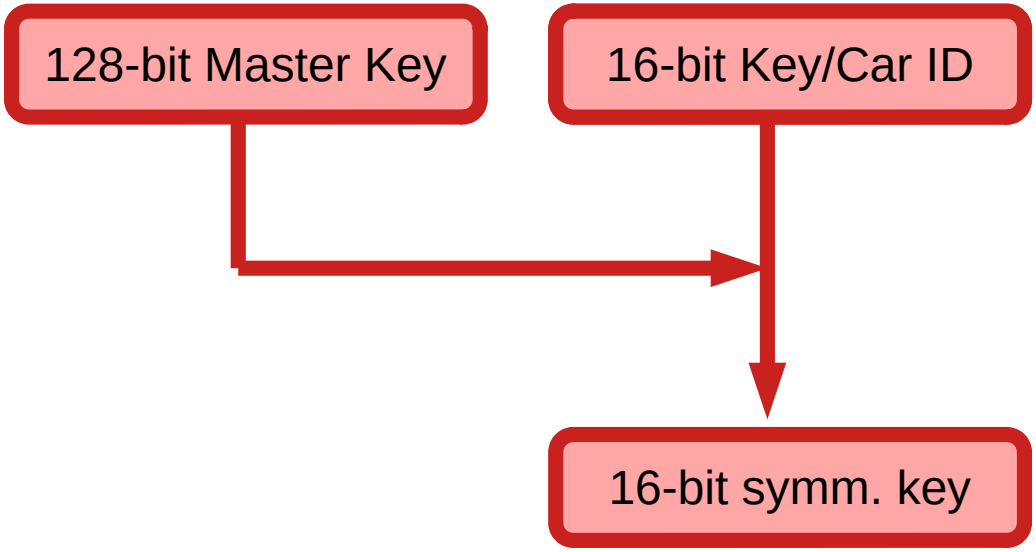
<valid token>

<valid token>

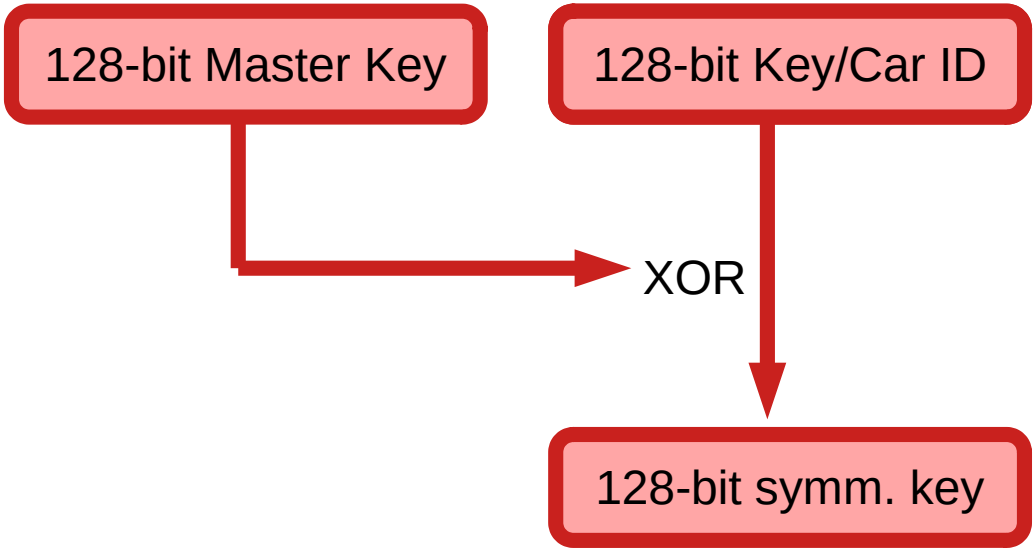
Nonce Scheme 3

```
if nonce != last_nonce+1:
  DENY
else:
  ACCEPT
  last_none = nonce
```

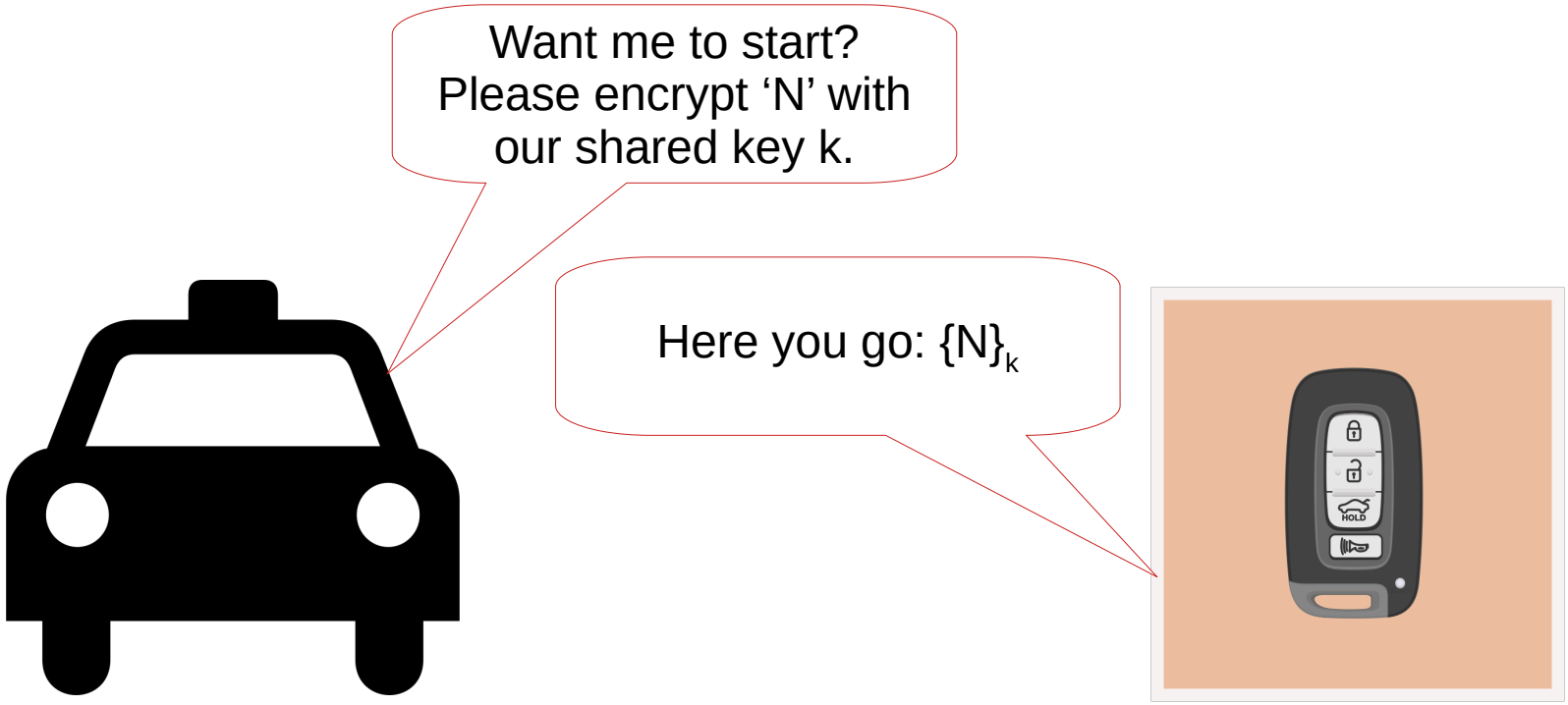
Cryptographic key diversification



Cryptographic key diversification

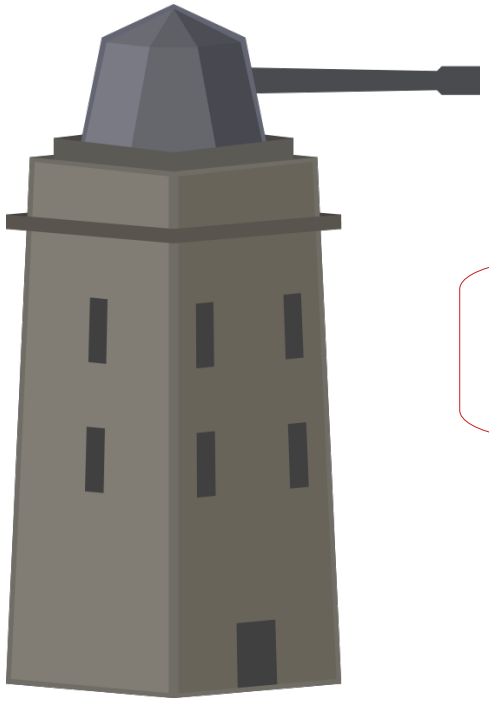


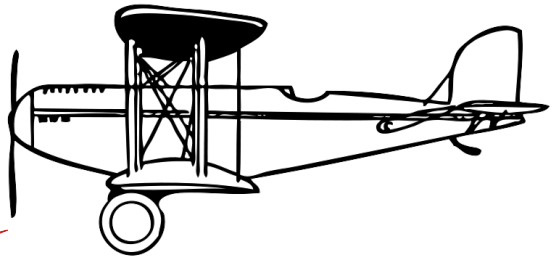
Inside the car: challenge-response protocol



Identify: Friend or Foe?

Identify: Friend or Foe?

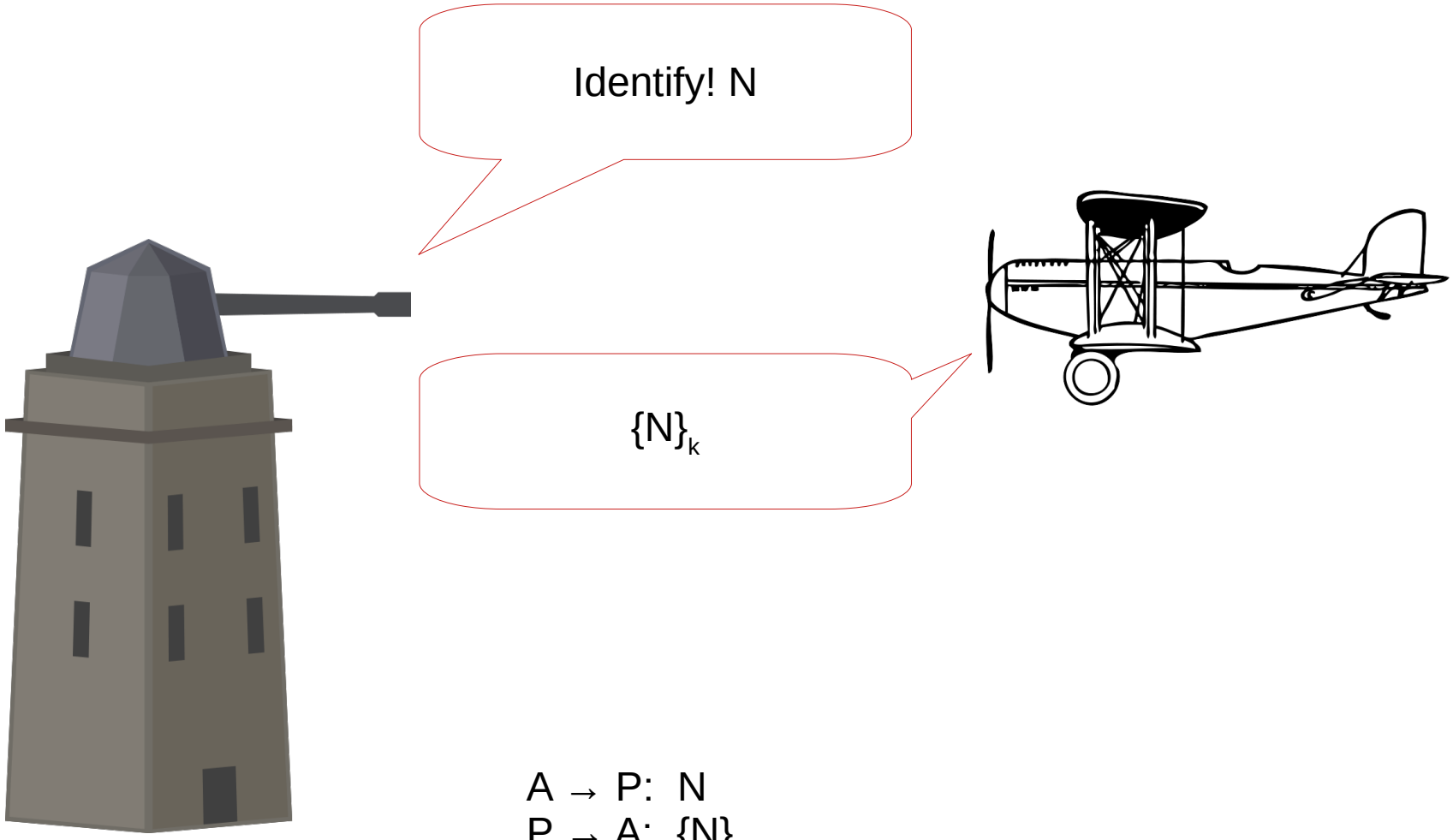




Don’t shoot!

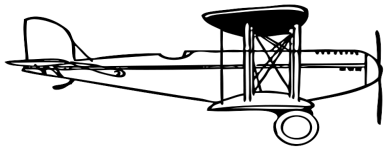
P → A: P

Identify: Friend or Foe?

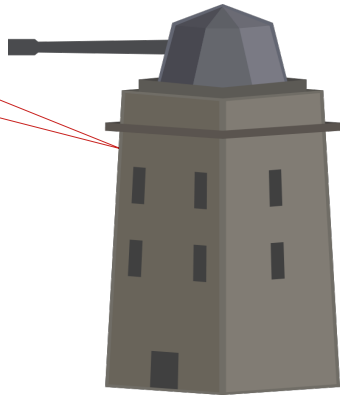


A → P: N
P → A: $\{N\}_k$

The MIG-in-the-middle



Identify! N

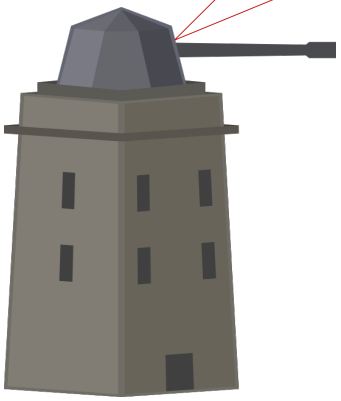


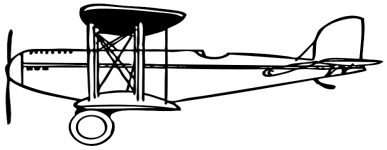
$\{N\}_k$

N?

{N}k

Identify! N





$\{N\}_k$

$A \rightarrow Q: \quad N$
$Q \rightarrow B: \quad N$
$B \rightarrow P: \quad N$
$P \rightarrow B: \quad \{N\}_k$
$B \rightarrow Q: \quad \{N\}_k$
$Q \rightarrow A: \quad \{N\}_k$

Man-in-the-middle

Buy “MLP: Friendship is Magic” for **£60**

This guy has **£60**?

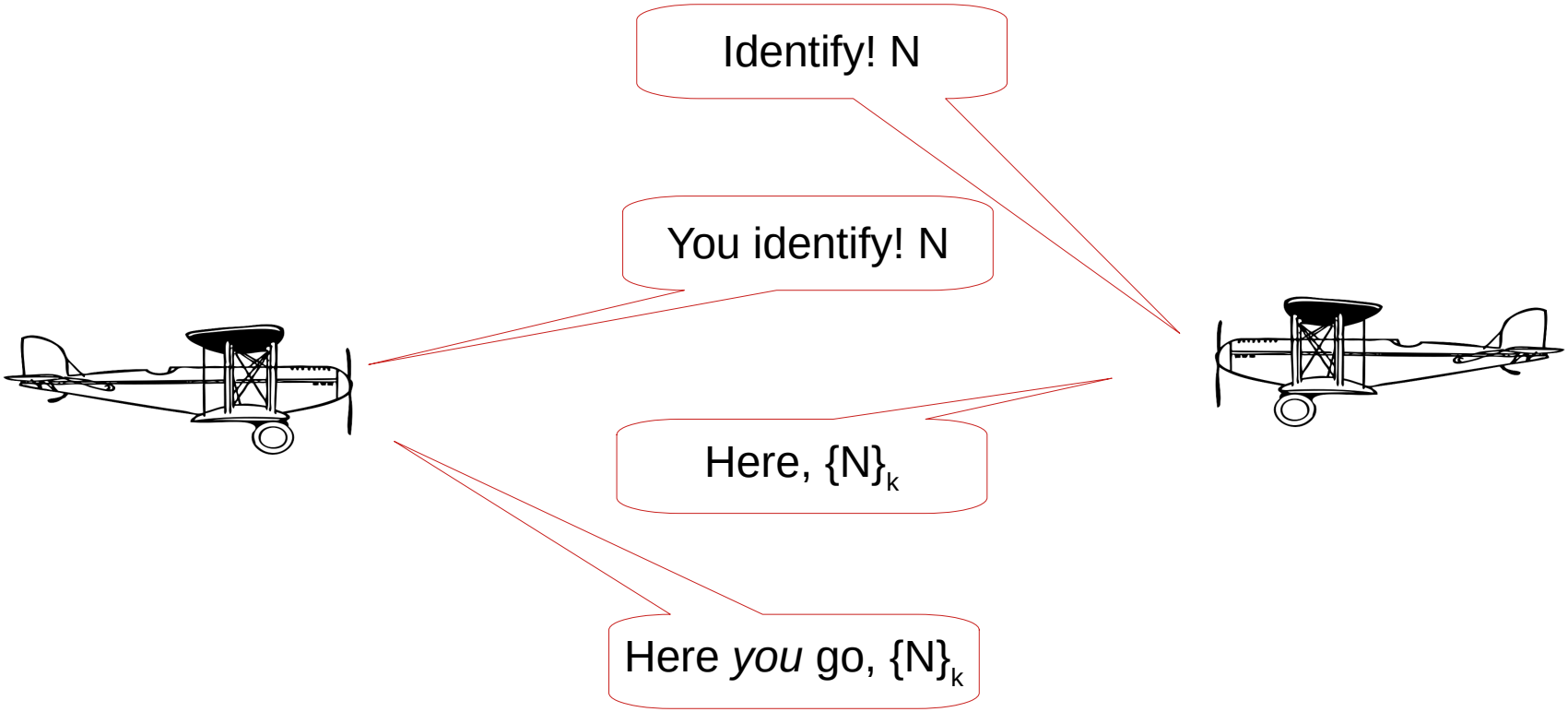
Man-in-the-middle

Man-in-the-middle

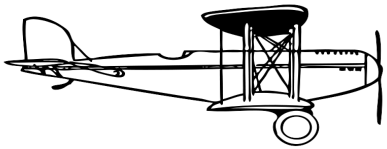
Buy “MLP: Friendship is Magic” for **£60**

This guy has **£6,000**?

Reflection attacks



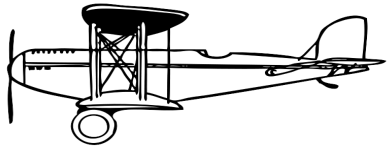
Reflection attacks



B

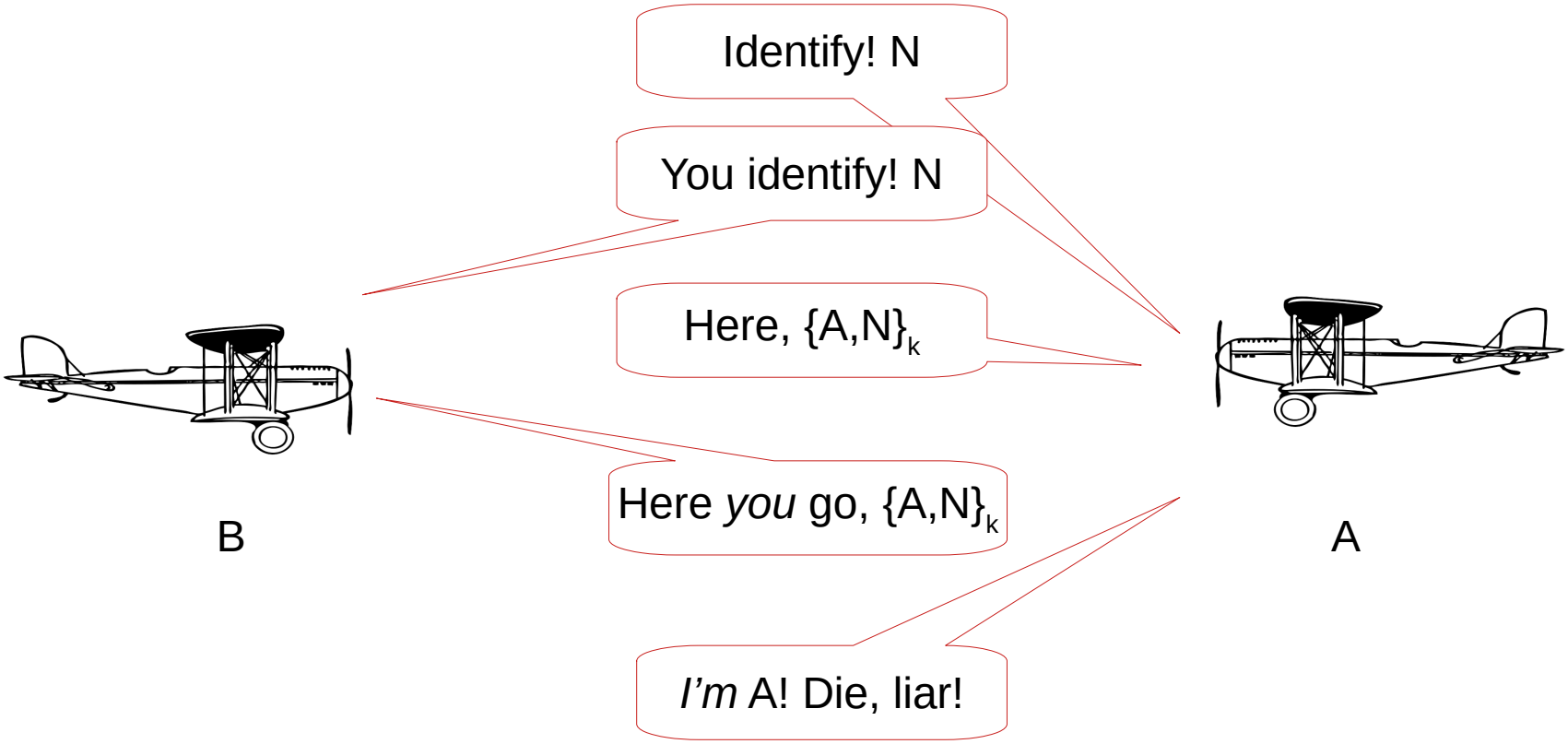
Identify! N

Here, $\{B,N\}_k$

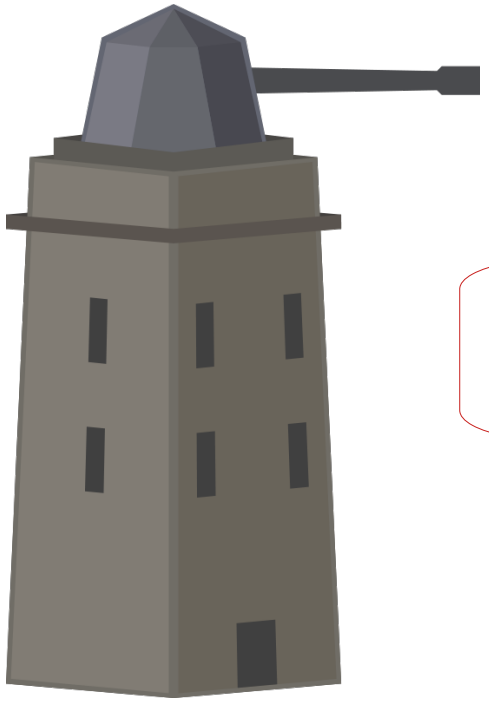


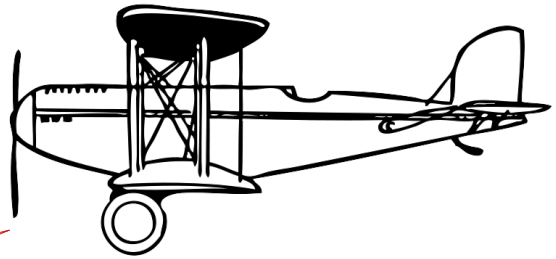
A

Reflection attacks



Announcing yourself

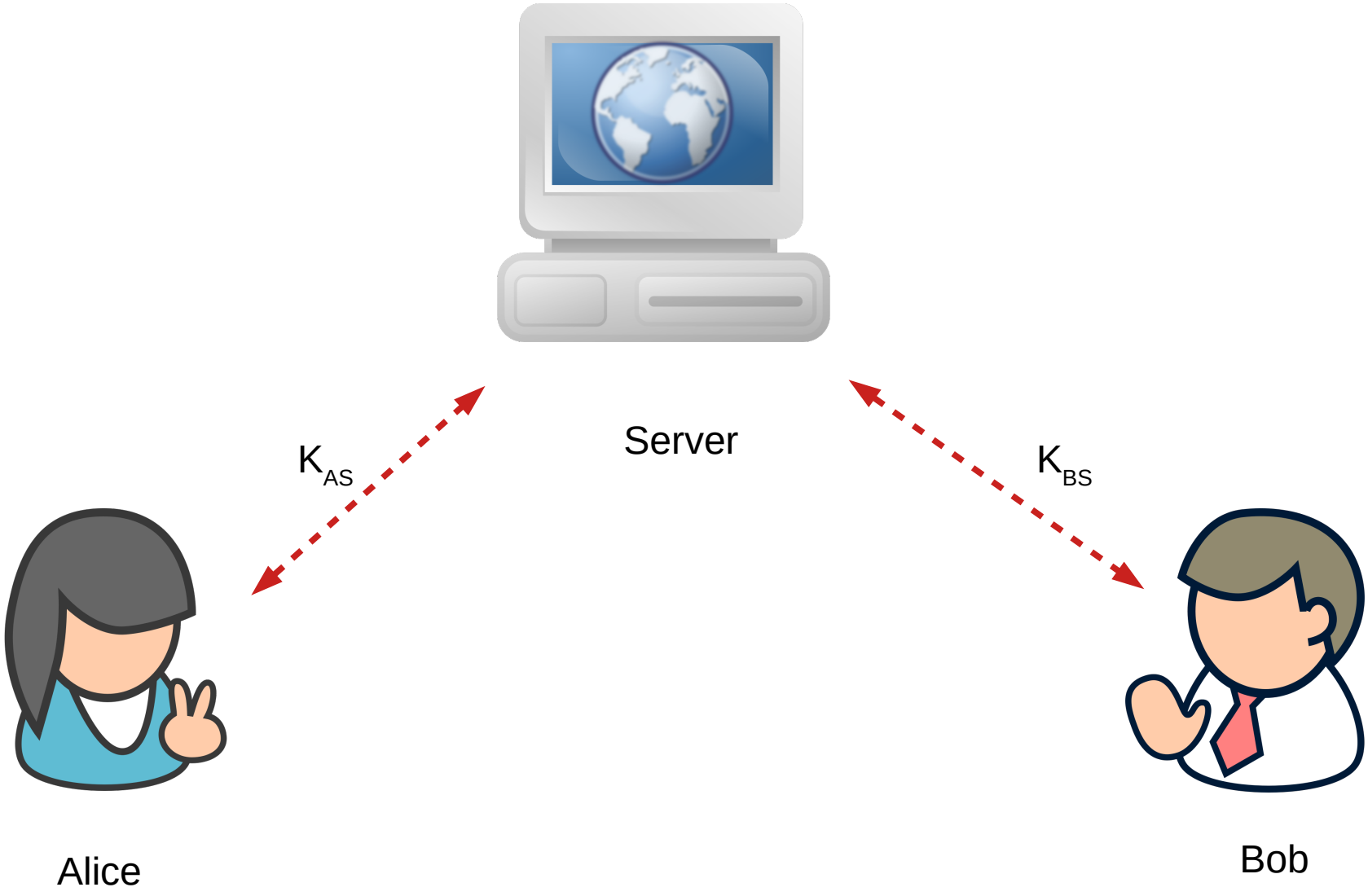




Don’t shoot!

P → A: P

Key Exchange


Server
K_{AS}
K_{BS}
Alice
Bob

Needham-Schroeder Protocol

Message 1 $A \rightarrow S : A, B, N_A$

Message 2 $S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{KBS}\}_{KAS}$

Message 3 $A \rightarrow B : \{K_{AB}, A\}_{KBS}$

Message 4 $B \rightarrow A : \{N_B\}_{KAB}$

Message 5 $A \rightarrow B : \{N_B - 1\}_{KAB}$

Needham-Schroeder Protocol

Message 1 $A \rightarrow S : A, B, N_A$

Message 2 $S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{KBS}\}_{KAS}$

3 years and 1 compromised key later….

Message 3 $!A \rightarrow B : \{K_{AB}, A\}_{KBS}$

Message 4 $B \rightarrow !A : \{N_B\}_{KAB}$

Message 5 $!A \rightarrow B : \{N_B - 1\}_{KAB}$

Needham-Schroeder Protocol

Message 1 $A \rightarrow B : A$

Message 2 $B \rightarrow A : \{A, N'_B\}_{KBS}$

Message 3 $A \rightarrow S : A, B, N_A, \{A, N'_B\}_{KBS}$

Message 4 $S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A, \underline{N'_B}\}_{KBS}\}_{KAS}$

Message 5 $A \rightarrow B : \{K_{AB}, A, \underline{N'_B}\}_{KBS}$

Message 6 $B \rightarrow A : \{N_B\}_{KAB}$

Message 7 $A \rightarrow B : \{N_B - 1\}_{KAB}$