CryptoCards

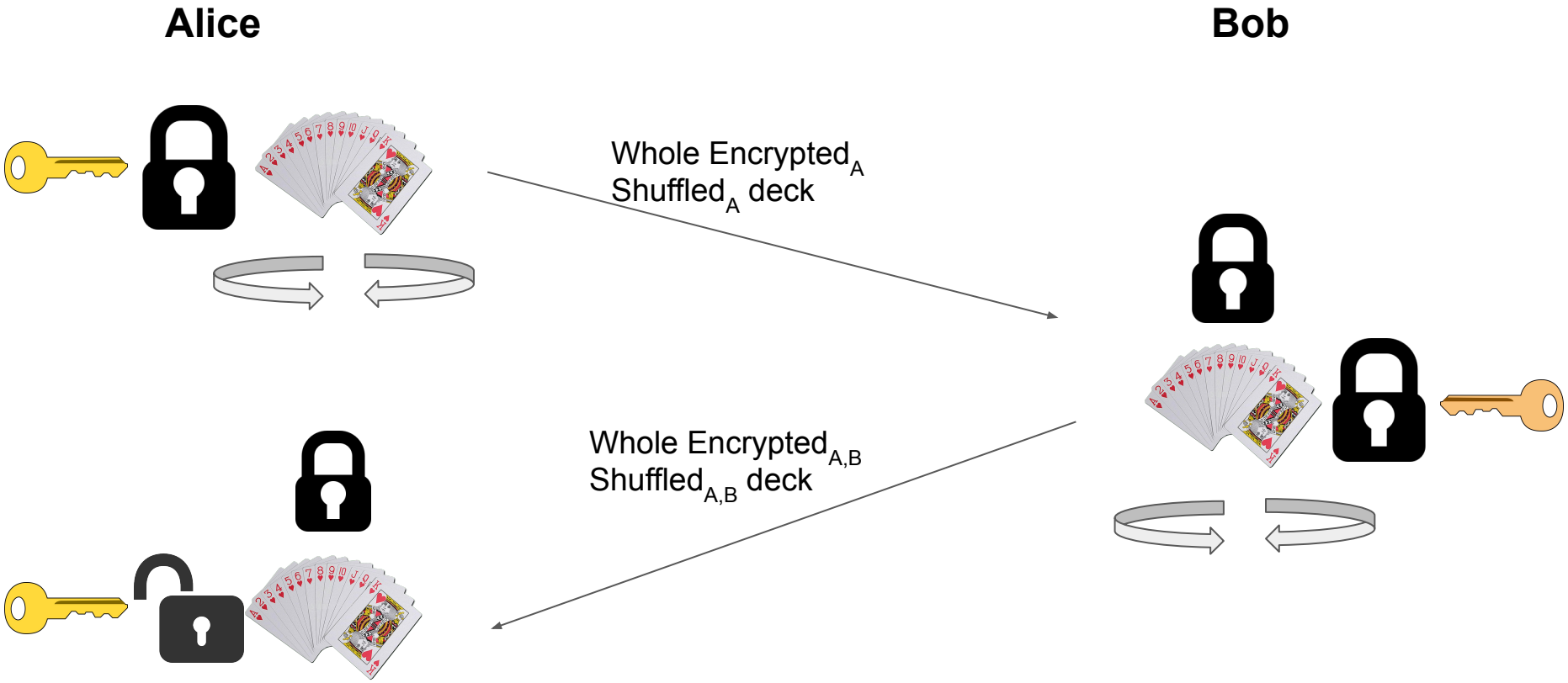
Pietro, Han, Lilly

The problem

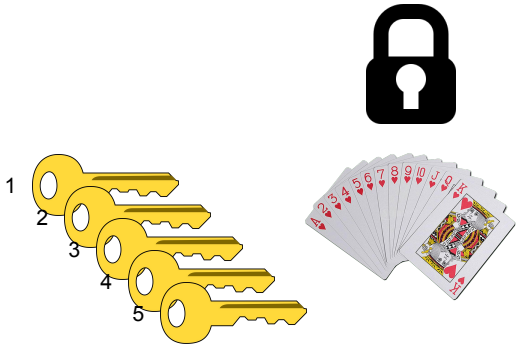
- Strangers don’t trust each other or the server

- How can players ensure each others’ cards are legitimate?

Suppose two player game...

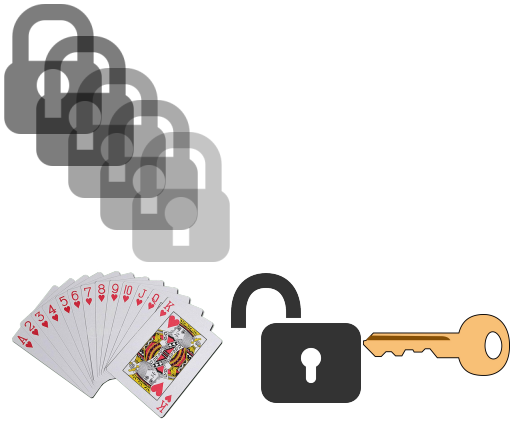

Alice
Bob
Whole Encrypted$_A$
Shuffled$_A$ deck
Whole Encrypted$_{A,B}$
Shuffled$_{A,B}$ deck

Alice



Whole Encrypted$_B$
Individually encrypted$_A$ deck

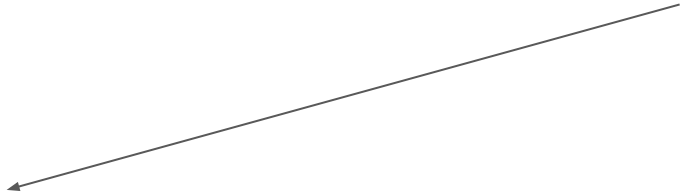
Bob

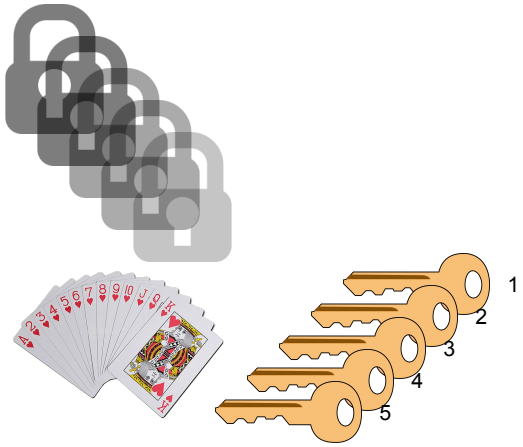


Alice

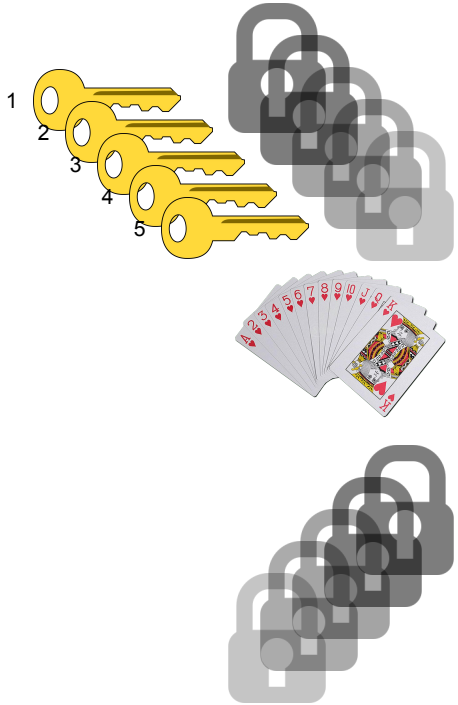
Bob

Individually encrypted$_{A,B}$ deck

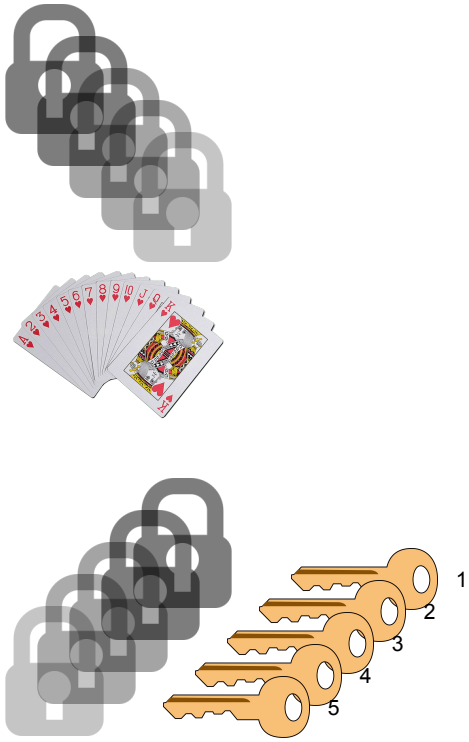




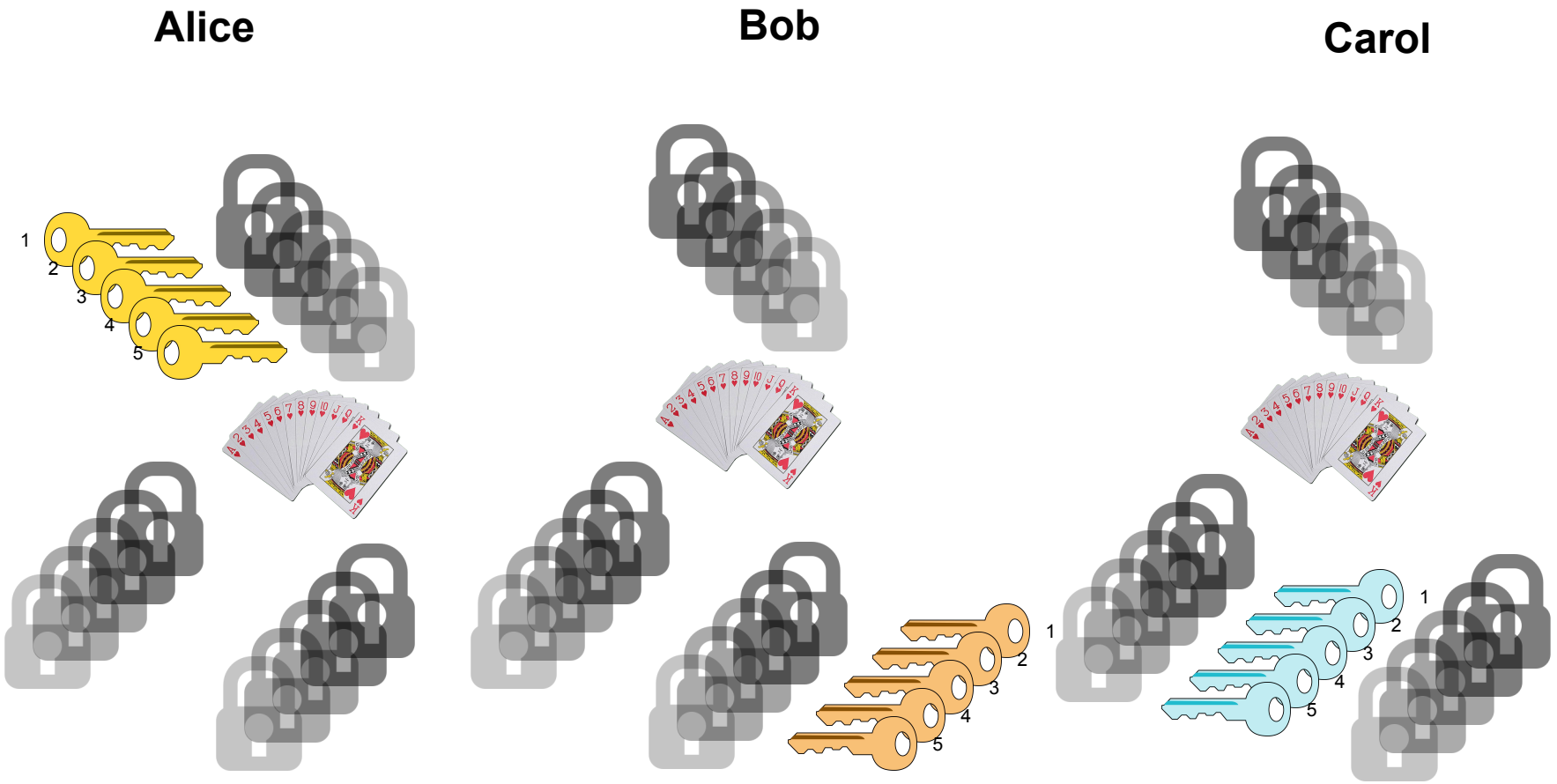
Alice



Bob



Suppose three players...


Alice
Bob
Carol
1
2
3
4
5
1
2
3
4
5
1
2
3
4
5

Repeat for x number of players

Problems with the solution

- Each additional player increases wait time linearly (+10 seconds per player, every round)
- Textbook RSA is commutative, but padding is not
  - Choosing smaller primes make encryption less secure, but decryption faster
  - Can decryption be done in the length of a blackjack game?
- Timeout feature is 1 day on the game instance

How quickly can a 1024-bit RSA be cracked?

- 2007: 700-bit RSA broken in 11 months
- 2010: 1024-bit RSA broken in 104 hours (81 Pentium 4 chips)
- 2015: 512-bit RSA broken in 4 hours ($75 dollar Amazon EC2 cloud instance)
- 2015: 1024-bit DH broken in 2 months (3000 CPUs by NSA)
- 2019: ???

Works Cited

https://ieeexplore.ieee.org/document/6043261 (GPU performance on 1024-RSA is superior, but not by the watt ratio)
https://www.ru.nl/publish/pages/769526/z_thesis_erikboss_final.pdf (112-bit ECDLP in 18.5 years, 1x GTX780/Radeon HD7850)
https://en.wikipedia.org/wiki/Key_size
https://www.theregister.co.uk/2015/10/19/nsa_crypto_breaking_theory/ (NSA breaks 1024-bit in 2 months using 3000 CPUs)

Code!