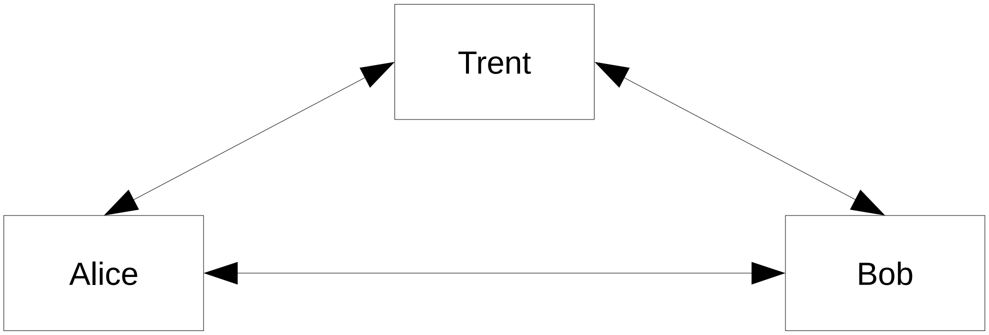
Cryptographic Protocols

protocol

- fundamentally, a series of steps to accomplish certain task
- must be:
  - known to everyone involved
  - agreed to by everyone involved
  - unambiguous
  - complete
  - explicit

types of protocols

- arbitrated
  - a third-party is involved to help prevent something from going wrong
  - this is a bit like prevention

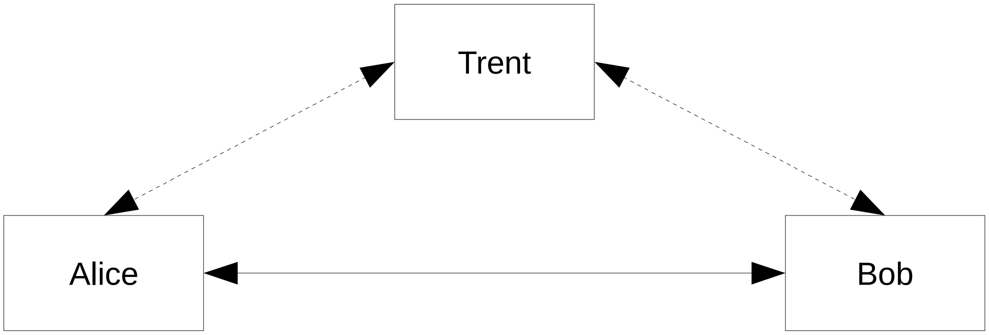


Alice wants to interact with Bob, but she does not trust him
Trent, a trusted arbitrator, plays a role by guaranteeing fairness during transactions
involving Trent is crucial and compulsory in this type of protocol

e.g.:

- Bob wants to buy a car from Alice
- Trent is a lawyer
- Bob gives money to Trent, and Alice gives the car title to Trent
- Trent verifies that both are appropriate and good
- Trent then passes those on to Alice and Bob respectively

- adjudicated
  - a third-party is involved *when required* to help verify if the protocol was followed correctly
  - this is a bit like detection



Alice and Bob perform transactions on their own, but then something goes wrong

Trent, a trusted party, gets involved
Trent evaluates the evidence presented by Alice and Bob, and decides whose fault it was
Trent's involvement is optional in this type of protocol

e.g.:
Bob wants to buy a car from Alice
Bob gives money to Alice, and Alice gives the signed car title to Bob
Alice later finds out that the money given to her was fake
She seeks help from a third-party, Trent (a judge or someone relevant)

self-enforcing
automatically guarantees fairness to all involving parties

no third-party is involved
the protocol design assures security and fairness

cryptographic protocol
a protocol that undertakes security-related functions
e.g., key generation, key exchange, authentication, etc
it does so by applying cryptographic methods

types of cryptographic protocols
key establishment protocol
keys may be distributed by a third-party trusted authority (TA)
keys may be established directly among the parties involved
e.g., Diffie-Hellman

e.g., interlock protocol
Alice sends her public key (K_{PA}) to Bob
Bob sends his public key (K_{PB}) to Alice
Alice encrypts her message using K_{PB} and sends half of the ciphertext to Bob
Bob encrypts his message using K_{PA} and sends half of the ciphertext to Alice
once both parties have received half of the ciphertext each, they send their other half

this helps to prevent man-in-the-middle attacks
an attacker has to wait for the entire ciphertext to decrypt it (half can't be decrypted)
security relies on the fact that each party must receive half before sending their other half

there are many other key establishment protocols

authentication protocol
deals with authenticating the parties involved in communication/transaction
a password and salt login system is an example
can also be done using public-key cryptography

e.g., SKEY password system (aka hash chaining)
choose a password, P, and hash it n times

$$H_1(P), H_2(H_1(P)), H_3(H_2(H_1(P))), \ldots, H_n(H_{n-1}(\ldots(P)))$$

Alice stores all the hash values and sends H_n to the server
the server stores H_n
to authenticate, Alice sends H_{n-1} to the server
the server hashes H_{n-1} and compares the hash value with H_n
if they match, the server authenticates Alice
    it also discards H_n and stores H_{n-1}
Alice uses H_{n-2} to login the next time
    she keeps doing this until she reaches H_1
once all the passwords have been exhausted, the process restarts

there are many other authentication protocols

attacks against protocols

- passive attack
    - involves an eavesdropper who observes the protocol to gain more information
- active attack
    - involves impersonating, introducing new messages, deleting existing messages, etc

- passive cheater
    - a participant who tries to get more information than what the protocol allows
- active cheater
    - a participant who tries to manipulate the protocol in order to cheat

hybrid cryptosystem

uses both symmetric and asymmetric cryptographic methods to secure a message
typically, the protocol uses asymmetric cryptography to securely exchange a symmetric key
symmetric cryptography is then used to actually transmit messages

asymmetric cryptography is computationally far more expensive
    so encrypting all messages using it may be infeasible
    it is usually only used to encrypt the key used for symmetric encryption

a last note

for any cryptosystem to work properly, all parties must abide by the rules of the protocol