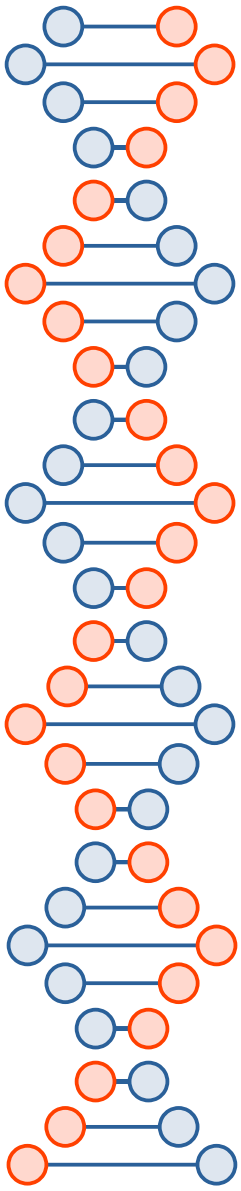
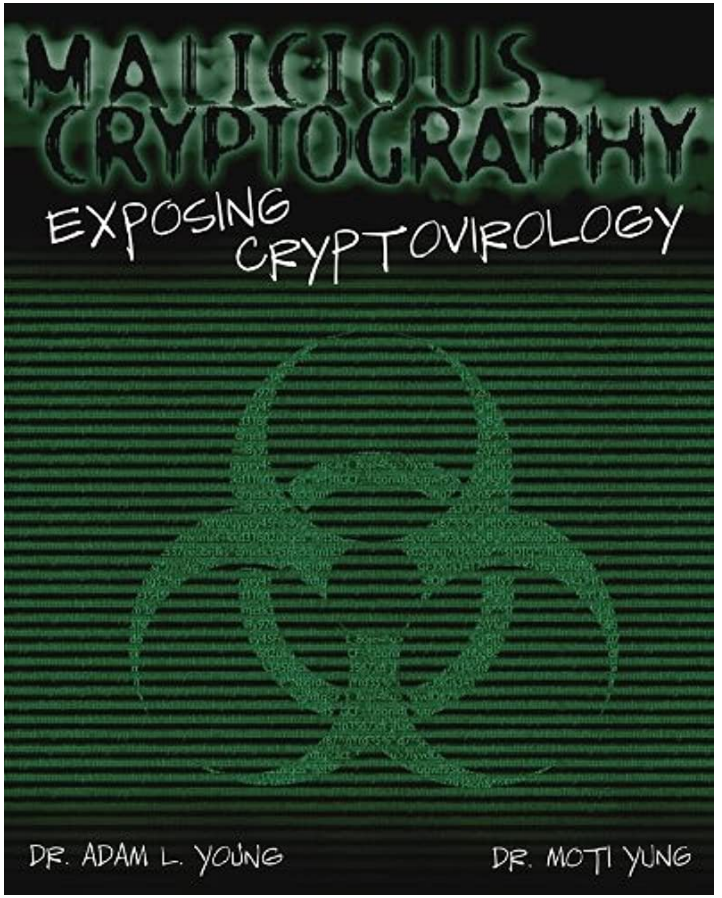


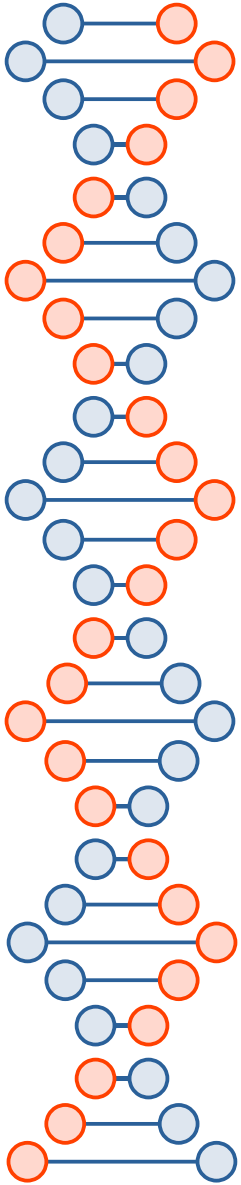
Zero Knowledge Proofs, Oblivious Transfer, ThreeBallot

CSE 539

jedimaestro@asu.edu

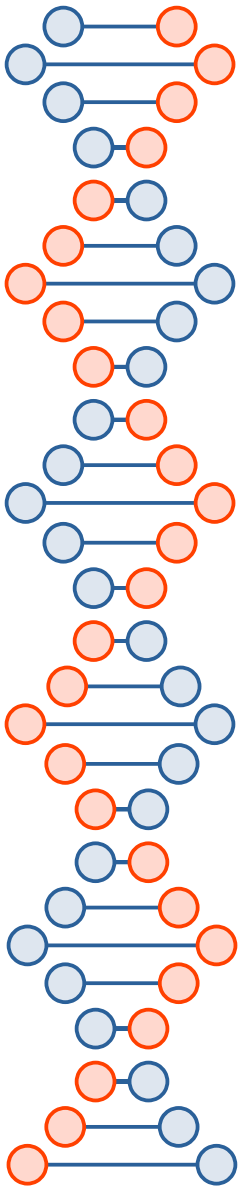
Crypto is more than just sending messages





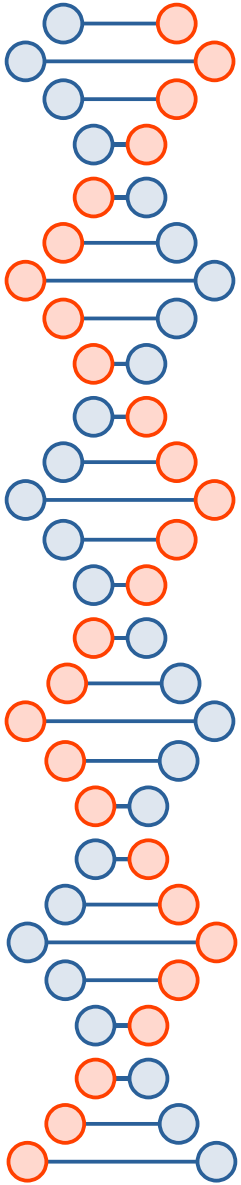
A sampling of topics

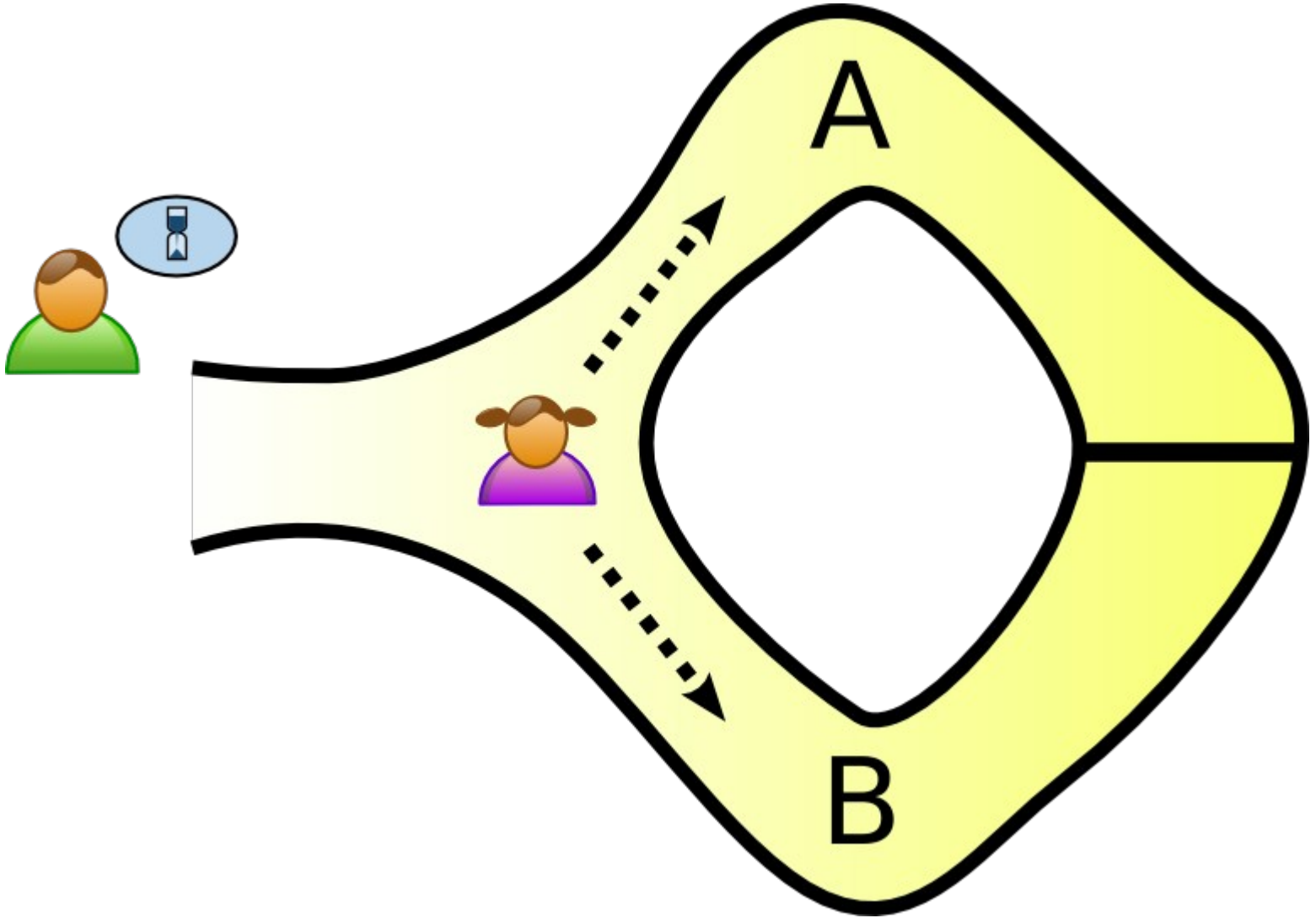
- Zero Knowledge Proofs
- Oblivious Transfer
- ThreeBallot

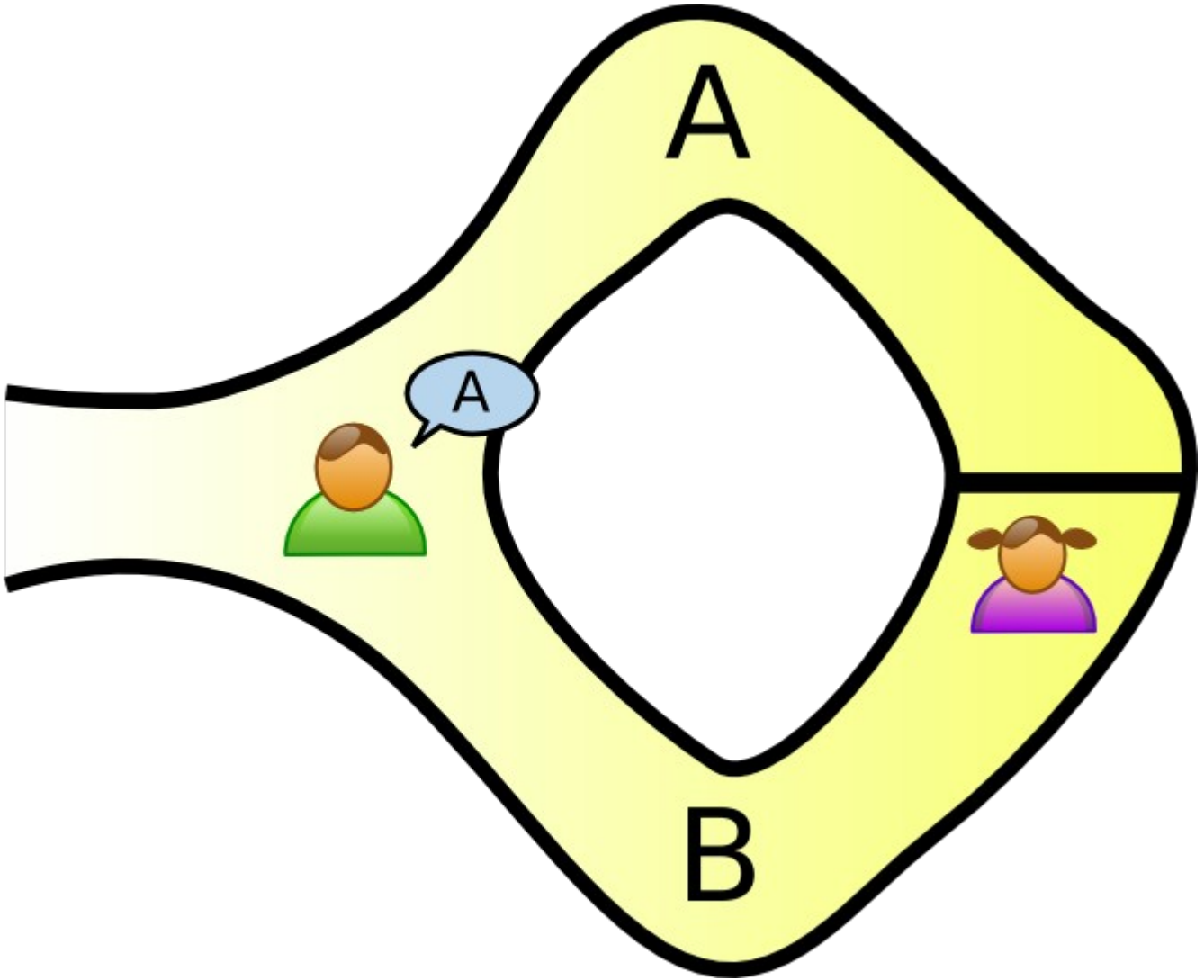


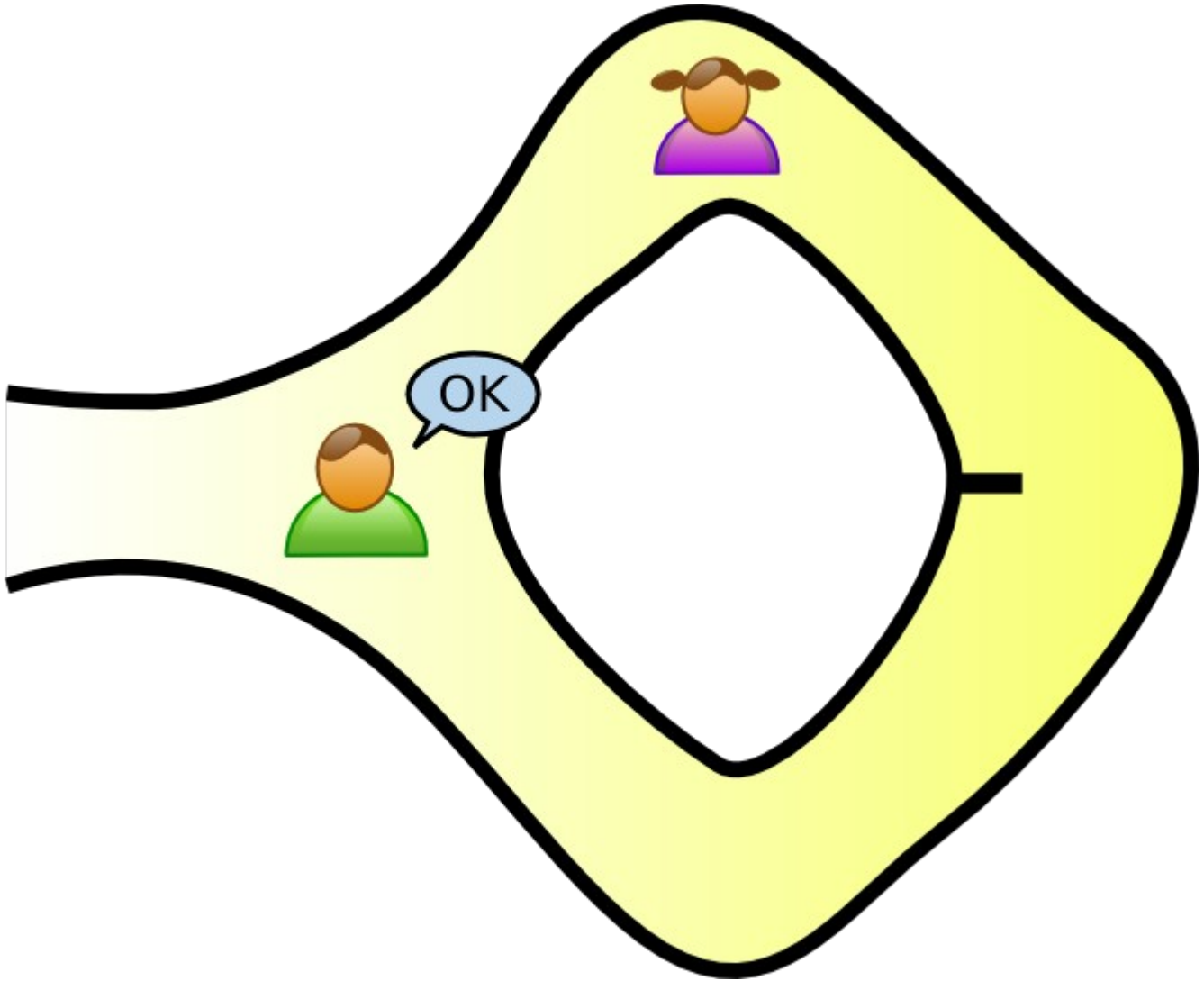
Zero Knowledge Proofs

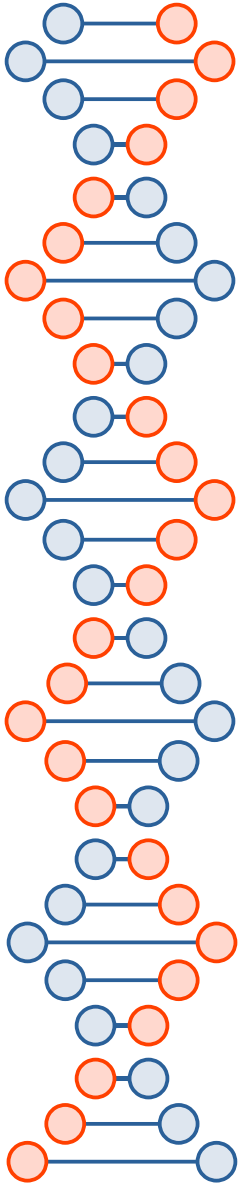
- “a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true”
  - https://en.wikipedia.org/wiki/Zero-knowledge_proof (also the source of the following images and examples)

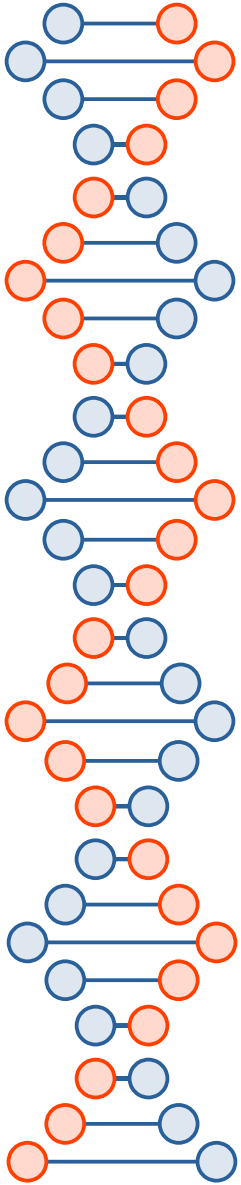



A
B


A
A
B

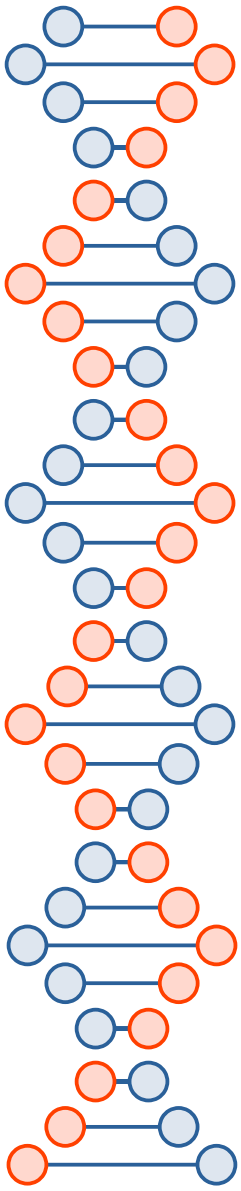

OK





Some definitions

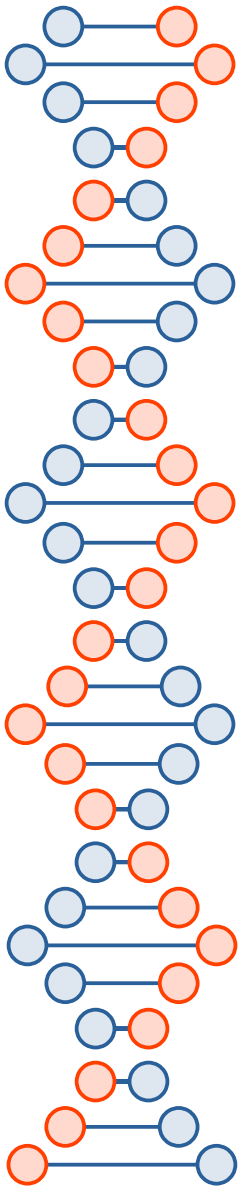
- “Completeness: if the statement is true, an honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.
- Soundness: if the statement is false, no cheating prover can convince an honest verifier that it is true, except with some small probability.
- Zero-knowledge: if the statement is true, no verifier learns anything other than the fact that the statement is true.”



Example with discrete log

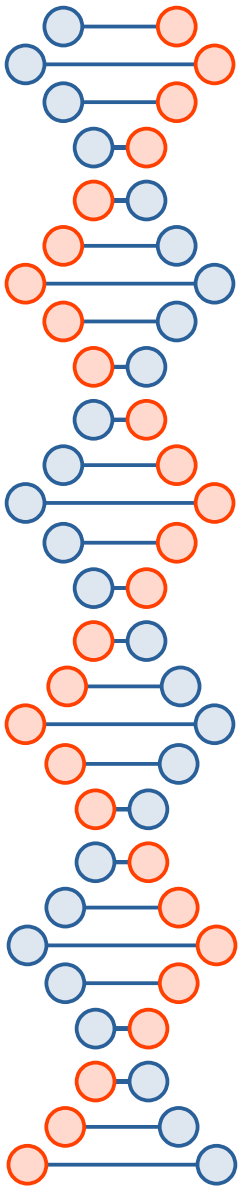
- $g^x \bmod p = y$
  - Peggy wants to prove she knows x
- Each round, Peggy computes $C = g^r \bmod p$
  - She generates r randomly
- In each round, Victor can ask for…
  - **r** --or--
  - **$(x + r) \bmod (p - 1)$**

$g^{(x + r) \bmod (p - 1)} \bmod p = g^x g^r \bmod p = Cy \bmod p$



Applications

- Signal’s anonymous credentials
- Blockchain
- Voting: verify your vote without revealing who you voted for
- Finance: verify your income is in a certain range
- Many more...

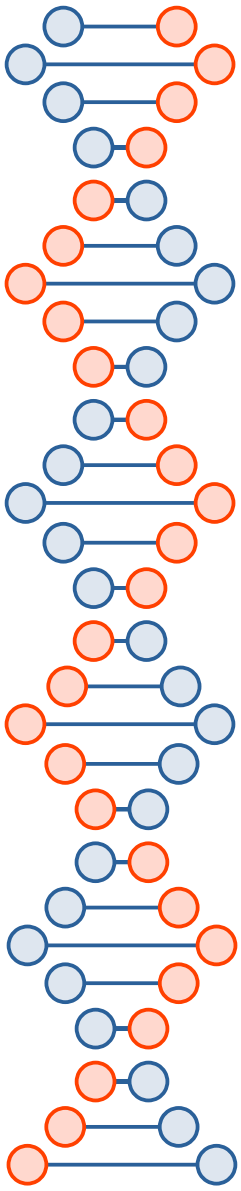


Oblivious Transfer

- Some background
  - Commitment scheme
    - Bob and Alice are getting a divorce (Coin Flipping by Telephone, *Manual Blum*)…
      - Hash(randomnumber, “heads”)
    - Can enforce randomness of bits
  - Mental poker

$$D(E(M)) \equiv (E(M))^d \equiv (M^e)^d \equiv M^{e*d} \pmod{n}$$
$$E(D(M)) \equiv (D(M))^e \equiv (M^d)^e \equiv M^{e*d} \pmod{n}$$

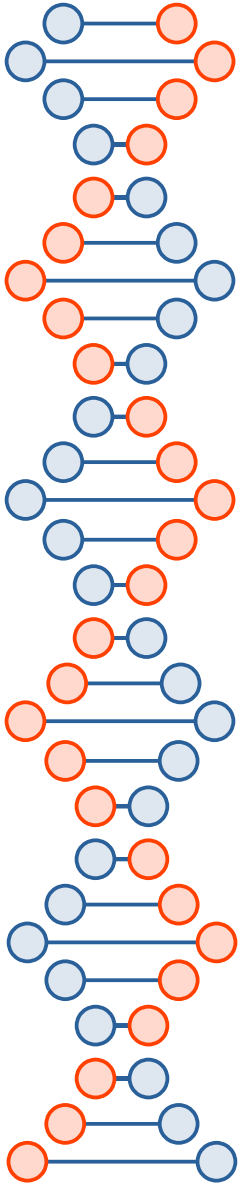
We’re moving in the direction of secure multiparty computation…



Oblivious Transfer

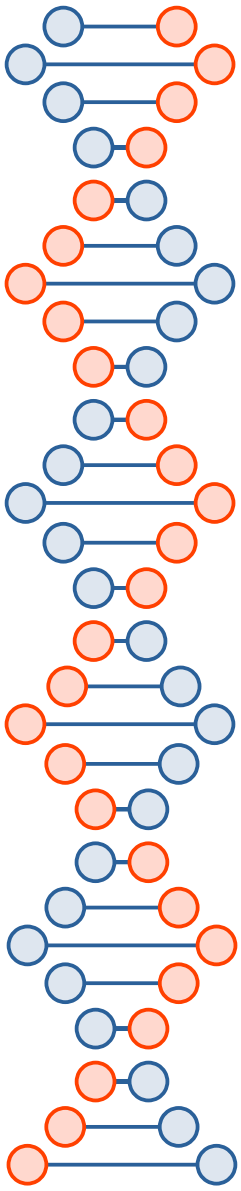
- *How to exchange secrets with oblivious transfer*, Rabin 1981
- Wikipedia: “an oblivious transfer (OT) protocol is a type of protocol in which a sender transfers one of potentially many pieces of information to a receiver, but remains oblivious as to what piece (if any) has been transferred.”
- “given an implementation of oblivious transfer it is possible to securely evaluate any polynomial time computable function without any additional primitive”

https://en.wikipedia.org/wiki/Oblivious_transfer



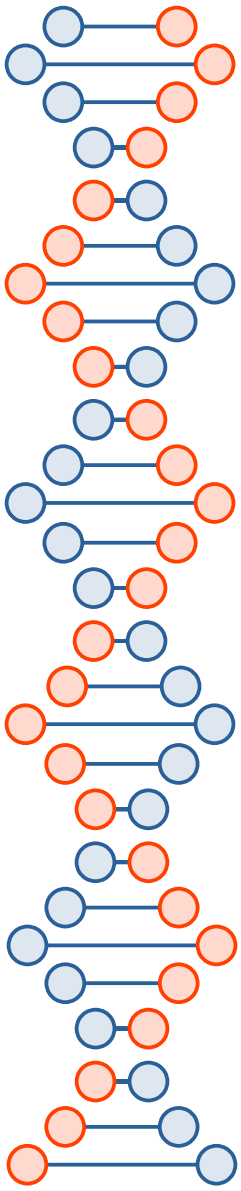
Alice has two messages: m_0 and m_1

- Alice wants to reveal only one of them to Bob
- Alice creates an RSA key pair
  - Keeps d
  - e and N are public
- Bob gets to choose which one (b = {0, 1}), also chooses a random number k
- Alice creates two random messages, x_0 and x_1
  - Both are public, sent to Bob



Bob makes public, i.e., sends to Alice...

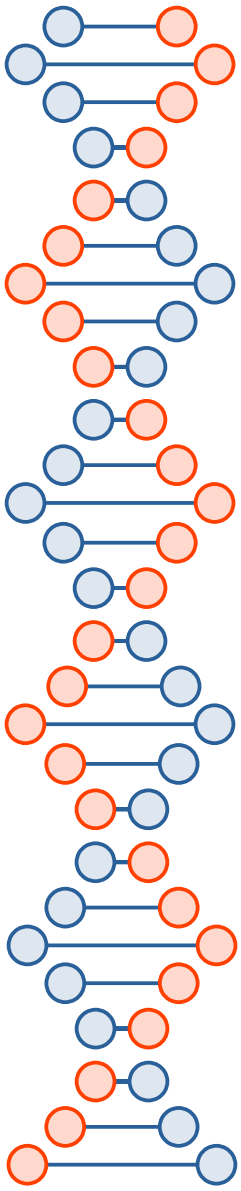
$$v = (x_b + k^e) \bmod N$$



Alice sends two replies...

$$k_0 = (v - x_0)^d \bmod N$$
$$k_1 = (v - x_1)^d \bmod N$$

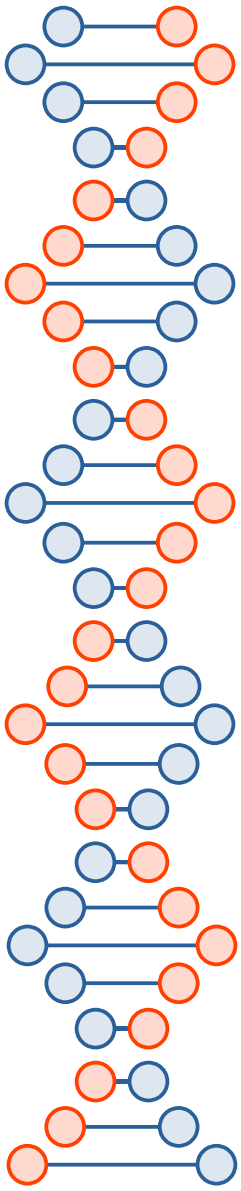
$$m'_0 = m_0 + k_0$$
$$m'_1 = m_1 + k_1$$



Bob decrypts…

$$m_b = m'_b - k$$

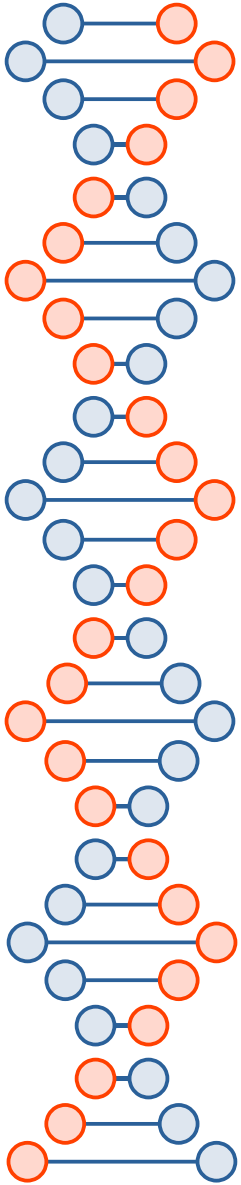
(The other m' is useless to him)



Why did it work?

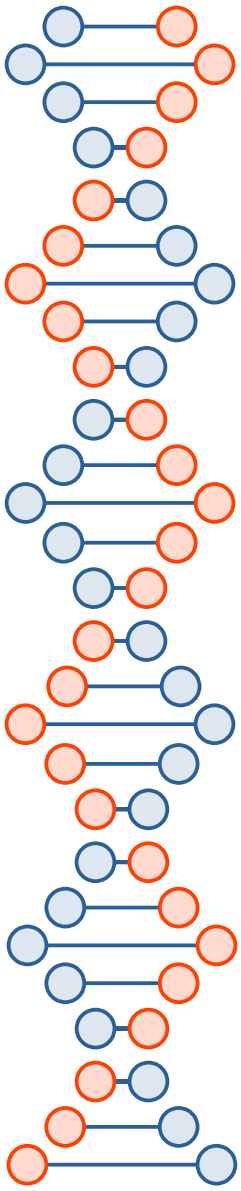
$$k_0 = (x_b + k^e - x_0)^d \bmod N$$
$$k_1 = (x_b + k^e - x_1)^d \bmod N$$

$$m'_0 = m_0 + k_0$$
$$m'_1 = m_1 + k_1$$



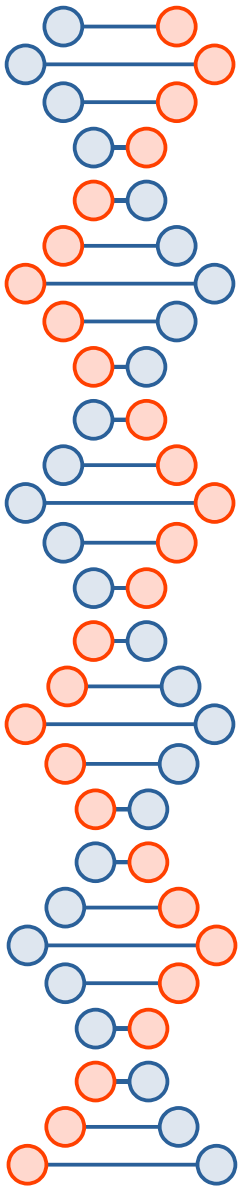
ThreeBallot (https://en.wikipedia.org/wiki/ThreeBallot)

- Proposed by Ron Rivest in 2006
- Voting principles in the U.S.
  - You should be able to verify your vote was counted correctly
  - You should not be able to prove to anybody who you voted for



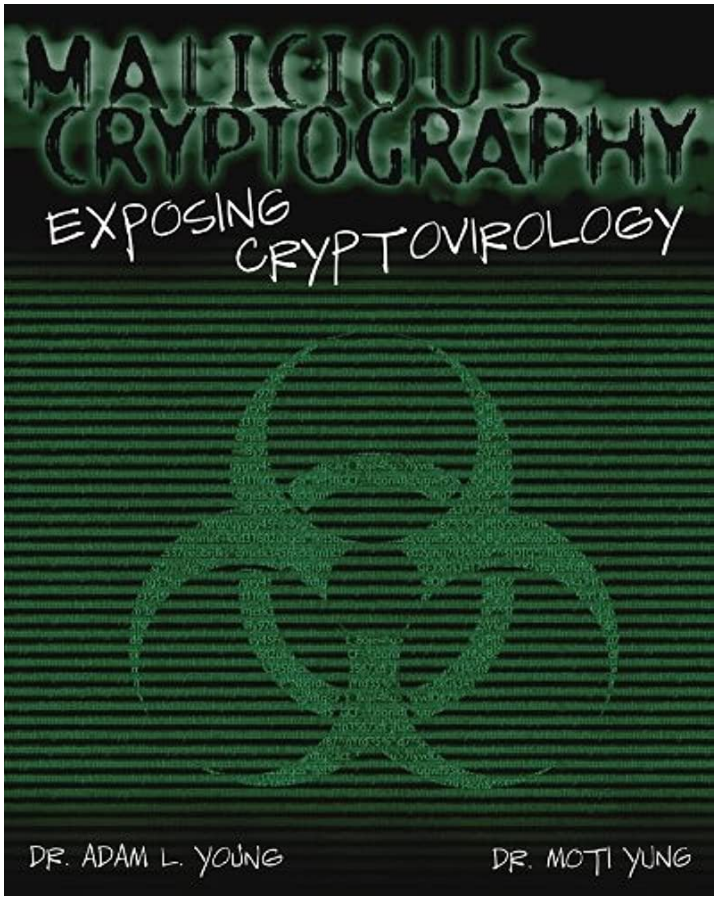
Candidate	Ballot			Notes
	1	2	3	
John Foo	X		X	Any two columns marked indicates a "for" vote.
Barb Bar			X	Any single column marked is not a "for" vote.
Bill Too		X		

Candidate	Ballot			Notes
	1	2	3	
Andy Oops	X	X	X	Not allowed.
Elle Error				Not allowed.



ThreeBallot

- All three ballots must be checked for compliance
  - Should vote twice for candidate you like, once for candidates you don’t
  - After this check, the entire stack of ballots should be shuffled
- The voter gets to track one ballot
  - 1/3 chance tampering with votes is detected by each voter
  - Number of votes that cancel out should be equal to the number of voters
- The voter can’t prove to anybody how they actually voted


MALICIOUS CRYPTOGRAPHY
EXPOSING CRYPTOVIROLOGY
DR. ADAM L. YOUNG
DR. MOTI YUNG