

## Oblivious Transfer

Alice will send Bob one of two messages. Bob will receive one. Alice won't know which one.

1. Alice generates two (RSA) public/private key pairs. She sends both public keys to Bob.

2. Bob chooses a DES key  $K$ . He chooses one of Alice's public RSA keys and enciphers  $K$  with it. He sends the encrypted key to Alice without telling her which of her public keys he used to encipher it.

3. Alice decrypts Bob's key twice, using both of her private RSA keys. In one case, she gets  $K$ . In the other case, she gets garbage which looks like a DES key. She can't tell which is which.

4. Alice encrypts the two messages with DES, one using  $K$  and the other using the garbage key. She sends both ciphertexts to Bob.

5. Bob tries to decrypt the two ciphertexts using  $K$ . He can read one message; the other is gibberish.

Alice doesn't know which message Bob can read. Alice could cheat unless we used the next step.

6. Alice gives Bob both of her private RSA keys so that he can verify that she did not cheat. After all, she could have encrypted the same message with both keys in Step 4.

### Simultaneous Contract Signing

Alice and Bob want to enter into a contract. They agree on it. Both want to sign, but neither wishes to sign unless the other signs as well.

One protocol uses a trusted arbitrator, Trent.

1. Alice signs a copy of the contract and sends it to Trent.

2. Bob signs a copy of the contract and sends it to Trent.

3. Trent sends a message to both Alice and Bob saying that the other has signed it.

4. Alice signs two copies of the contract and sends them to Bob.

5. Bob signs both copies, keeps one and sends the other to Alice.

6. Alice and Bob both tell Trent that they each have a copy of the contract signed by both of them.

7. Trent destroys the two copies of the contract that he has.

What if Alice and Bob had no arbitrator, but were face-to-face?

1. Alice signs the first letter of her name on two copies of the contract and hands them to Bob.
2. Bob signs the first letter of his name on both copies and hands them back to Alice.
3. Alice signs the second letter of her name on both copies and hands them back to Bob.
4. Bob signs the second letter of his name on both copies and hands them back to Alice.
5. This continues until Both Alice and Bob have signed their entire names.

What if Alice and Bob had no arbitrator, and were not face-to-face?

Then they exchange a series of signed messages of the form, "I agree that with probability  $p$ , I am bound by this contract."

Suppose that Alice doesn't want to be bound to the contract with a probability more than 2% higher than the probability Bob is bound. Suppose also that Bob doesn't want to be bound to the contract with a probability more than 3% higher than the probability Alice is bound.

1. Alice and Bob agree on a time by which the signing protocol should be completed.
2. Alice sends Bob a message with  $p = 0.02$ .
3. Bob sends Alice a message with  $p = 0.05$ .
4. Alice sends Bob a message with  $p = 0.07$ .
5. Bob sends Alice a message with  $p = 0.10$ .
6. These steps alternate until both have received messages with  $p = 1$  or else the time in Step 1 has passed.

What if Alice and Bob had no arbitrator, and were not face-to-face, and couldn't agree on the probabilities above?

1. Both Alice and Bob randomly select  $2n$  DES keys, in pairs.
2. Both Alice and Bob generate  $n$  pairs of messages:  $L_i =$  "This is the left half of my signature."  $R_i =$  "This is the right half of my signature." Each message also contains a digital signature of the contract and a time stamp. The contract is considered signed by a party if both  $L_i$  and  $R_i$  can be produced for some  $1 \leq i \leq n$ .
3. Both Alice and Bob encrypt their message pairs using the  $2n$  DES pairs, the left message with the left key and the right message with the right key.
4. Alice and Bob send each other their pile of  $2n$  encrypted messages, making it clear which is which.

5. For  $1 \leq i \leq n$ , Alice and Bob send each other one of the keys in the  $i$ -th pair by oblivious transfer, omitting Step 6 for now. Now they each have one key in each pair, but neither knows which signature halves the other can read.

6. Both Alice and Bob decrypt the messages they can, using the keys they received. They check that the messages are valid.

7. Alice and Bob send each other the first bits of all  $2n$  DES keys.

8. Alice and Bob repeat Step 7 for the second, third, etc., bits, until all bits of all the DES keys have been exchanged.

9. Alice and Bob decrypt the remaining halves of the message pairs and the contract is signed.

10. Alice and Bob exchange the private RSA keys (Step 6 of oblivious transfer) and verify that the other has not cheated.