Class 25: Cryptography

Schedule

Lighting of the Lawn is **tonight**! (Starts around 7pm)

If you would like to present something to the class, you need to submit **Problem Set Omega** by **Sunday, 4 December** at **6:29pm**. Your submission should include an answer to "Presentation option" question:

> Presentation option: if you would like to present in class Tuesday, write a brief explanation of what you would like to do and how much time you are requesting for it. You can also include anything you want to make a compelling case for why your project should be selected (depending on how many requests for presentation their are, it may be necessary to select only as many as fit into the class).

Your final (optional) submission is due **Tuesday, 6 December**. You may revise and update earlier submissions until this deadline.

The **final exam** is scheduled by the registrar for **Saturday, 10 December, 9am-noon** in our normal classroom. See the Final Exam Preparation handout for more information and some **practice problems**.

Symmetric Cryptography

Correctness: $D(K, E(K, M)) = M$

Security: without K, it is hard to learning anything interesting about M from $E(K, M)$.

Why is $\oplus$ (xor) such a useful operator for cryptography?

Perfect cipher (Claude Shannon, 1940s). The ciphertext reveals no information (other than maximum length) about the plaintext.

Why must a perfect cipher have $|K| \geq |M|$? (K is the set of possible keys, M is the set of plaintext messages)

Why is a one-time pad impractical for most purposes? How do you break a "two"-time pad?

Asymmetric (Public Key) Cryptography

> *We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.*
> Whit Diffie and Martin Hellman, *New Directions in Cryptography*, November 1976

Primitive root. α is a primitive root of q if $\forall 1 \leq n < q. \exists m, 1 \leq m < q$ such that $\alpha^m = n \mod q$. All prime numbers have primitive roots.

Diffie-Hellman-Merkle Key Agreement

Goal: Alice and Bob agree on a secure key K, over an insecure channel with no prior agreement.

Assumption: Discrete log problem is hard (for sufficiently large inputs).

1. Choose and public the public parameters:
   q, large prime number α, primitive root of q
2. Alice generates random X_A.
3. Alice sends $Y_A = \alpha^{X_A} \mod q$.
4. Bob generates random X_B.
5. Bob sends $Y_B = \alpha^{X_B} \mod q$
6. Alice computes $K = (Y_B)^{X_A} \mod q$ / Bob computes $K = (Y_A)^{X_B} \mod q$.

How do we know Alice and Bob will agree on the same key, K?

What would an eavesdropper need to do to learn K?

Secure Multi-Party Computation

How can we compute a stable matching without revealing sensitive preferences?

