CS Bits & Bytes
Highlighting Innovative Computer Science Research

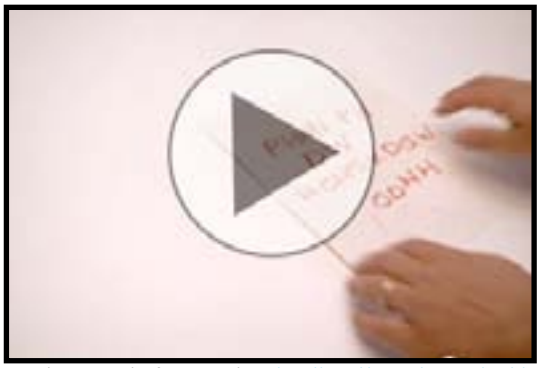
CS Bits & Bytes is a bi-weekly newsletter highlighting innovative computer science research. It is our hope that you will use CS Bits & Bytes to engage in the multi-faceted world of computer science to become not just a user, but a creator of technology. Please visit our website at: http://www.nsf.gov/cise/csbytes.

December 3, 2012
Volume 2, Issue 7

Cryptography

From online holiday shopping to emailed season's greetings, the Internet is used to transmit vast quantities of personal and financial information. Have you ever wondered what keeps your information safe? It's all about **cryptography!**

MUST SEE!



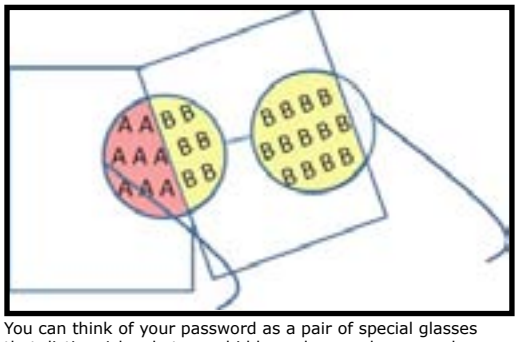
See a basic example of cryptography at:http://www.khanacademy.org/math/applied-math/crypt/v/intro-to-cryptography

Cryptography provides techniques for securing communication in the presence of third party adversaries. One of the fundamental problems in cryptography is the need to prove an identity to perform a transaction, while also keeping that identifying information private.

Luckily, computer science researchers devised a way to do this! The methods ensure that no one listening in to the interaction between you and the recipient or even the legal recipient himself, can later pretend to be you and engage in "identity theft." Because no secret knowledge is revealed, this approach is called a "zero-knowledge proof." Zero-knowledge proofs are used throughout cryptography and are crucial for secure electronic identity verification.

In practice, this is done by verification of the sender's ability to perform challenging computations that would be impossible without knowing the secret information— be it an account number or password. The challenging computations that the sender is asked to perform are chosen at random by the recipient, so it will be extremely unlikely that the same challenge would be repeated the next time the sender needs to prove its identity. Although these computations are difficult without knowing the secret information, it is easy to verify that they were done correctly even without the secret information.

The process can be illustrated using the analogy of an exchange between two people, who for zero-knowledge proofs are commonly labeled as: Peggy, the prover/sender, and Victor, the verifier/recipient. Say Peggy wants to convince Victor that she has special glasses (analogous to the password) that enable her to distinguish between colors A and B that Victor cannot tell apart. Peggy hands to Victor two pieces of paper which are identical to each other in all ways except that the first one is colored A and the second is colored B. Of course, to Victor the pages look identical.. Victor goes off and tosses a coin. If the coin comes up heads, he returns to Peggy the first paper she handed to him; if the coin comes up tails, he returns to Peggy the second paper she handed to him. In other words, if his coin was heads, Peggy gets the paper colored A, or, if it was tails, she gets back the paper colored B. Now Peggy uses her special glasses to tell which colored paper she got back, and lets Victor know if it's colored A or B. If she answers correctly, Victor believes Peggy has the special glasses, otherwise he does not.



You can think of your password as a pair of special glasses that distinguishes between hidden colors, and password verification as correctly identifying a hidden color for another person without giving them your glasses!

Let's dive deeper into this scenario. If Peggy did not actually have the glasses (analogously, if she did not know the password), there would only be a 50% chance that she'd be able to know which color page she got back since she would have to correctly guess the outcome of Victor's coin toss to name the right color. Even if she were able to guess correctly, repeating the process many times would ultimately reveal that she does not have the glasses as the chance that she could repeatedly guess Victor's coins would be small after a number of repetitions.

Professor Shafrira Goldwasser

It is easy for computers to repeat a verification routine many times and efficiently establish the validity of the Prover with an extremely high certainty, preventing impersonators from getting through.

Who Thinks of this Stuff?! Shafrira "Shafi" Goldwasser, RSA Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology (MIT), has been called one of the founders of modern cryptography. She co-invented zero-knowledge proofs with Silvio Micali and Charles Rackoff in the 1980's, and currently co-chairs MIT's Cryptography and Information Security Group. When she's not finding new ways of protecting information, Shafi enjoys reading, swimming, and participating in a playback acting troupe.

Links:

Read more about the MIT Cryptography and Information Security Group at: http://groups.csail.mit.edu/cis/.

An alternate explanation of zero-knowledge proofs can be found at: http://pages.cs.wisc.edu/~mkowalcz/628.pdf.

A variety of cryptography games are under development at: http://www.cryptoclub.org/.

Activity:

In the above scenario, if Peggy does not actually have the special glasses, she has a 50/50 chance of guessing the color correctly – the same odds as correctly guessing Victor's coin flip.

As a class, calculate the probability of correctly guessing the outcome of a coin flip n times in a row. Make a table on the board.

n	Odds of guessing correctly every time	
	2-sided coin	3-sided coin
1		
2		
3		
4		

Discussion Topic 1: How many correct outcomes in a row would Peggy need to have in order to convince you that she has the glasses?

Discussion Topic 2: What are the advantages of using a computer algorithm to carry out a zero-knowledge proof?

Discussion Topic 3: What if we used glasses that can distinguish three colors from each other, which were impossible for Victor to distinguish (imagine a three-sided coin)?

CS BITS & BYTES
http://www.nsf.gov/cise/csbytes/
Please direct all inquiries to: csbitsandbytes@nsf.gov

National Science Foundation
Computer & Information Science & Engineering Directorate
4201 Wilson Blvd Suite 1105
Arlington VA, 22230