

Spring Quarter of 2011 Special Topics in Computer Science:

Cryptography

Prof. Phillip Rogaway - rogaway@cs.ucdavis.edu

CRN 53390 - 4 Units MWF 2:10 - 3:00 pm Room: 146 Robbins

This year the CS Department will, for the first time, offer an undergraduate class in cryptography — the science of secure communications. We'll talk about encryption, authentication, and protocols. Cryptography can be hard, but I'll do my best to make it accessible. Prereqs are a suspicious disposition and a level of sophistication in math and computer science consistent with being a junior or senior in CS, CSE, or Math.

I'M SURE YOU'VE HEARD ALL ABOUT THIS SORDID AFFAIR IN THOSE GOSSIPY CRYPTOGRAPHIC PROTOCOL SPECS WITH THOSE BUSYBODIES SCHNEIER AND RIVEST, ALWAYS TAKING ALICE'S SIDE, ALWAYS LABELING ME THE ATTACKER.



YES, IT'S TRUE. I BROKE BOB'S PRIVATE KEY AND EXTRACTED THE TEXT OF HER MESSAGES. BUT DOES ANYONE REALIZE HOW MUCH IT HURT?



HE SAID IT WAS NOTHING, BUT EVERYTHING FROM THE PUBLIC-KEY AUTHENTICATED SIGNATURES ON THE FILES TO THE LIPSTICK HEART SMEARED ON THE DISK SCREAMED "ALICE."



 \tilde{E}_{K}^{N1}

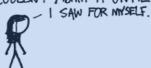
I DIDN'T WANT TO BELIEVE.

OF COURSE ON SOME LEVEL.

I REALIZED IT WAS A KNOWNPLAINTEXT ATTACK. BUT I

COULDN'T ADMIT IT UNTIL.

I SAW FOR MYSELF



SO BEFORE YOU SO QUICKLY LABEL
ME A THIRD PARTY TO THE COMMUNICATION, JUST REMEMBER:

1 LOVED HIM FIRST. WE
HAD SOMETHING AND SHE
/ TORE IT AWAY. SHE'S
THE ATTACKER, NOT ME.



NOT EVE.

Auth