Preparing for the Final

MATH 481/581 — Cryptography
Wednesday, May 2

Please print your name:

Bonus challenge. Let me know about any typos you spot in the posted solutions (or lecture sketches). Any typo, that is not yet fixed by the time you send it to me, is worth a bonus point.

Problem 1. The final exam will be comprehensive, that is, it will cover the material of the whole semester.

(a) Do the practice problems for both midterms.

(b) Do the problems below. (Solutions will be posted soon.)

Problem 2. We use the (silly) hash function $H(x) = x \pmod{25}$.

Alice's public RSA key is $(N, e) = (55, 13)$, her private key is $d = 17$.

(a) How does Alice sign the message $m = 3141592$?

(b) How does Bob verify her message?

(c) Verify whether the message $(m, s) = (1234, 9)$ was signed by Alice.

(d) Give an example of a collision of our hash function.

Problem 3.

(a) Does Alice have to choose a new y if she sends several messags to Bob using ElGamal? Explain!

(b) The movie "Swordfish" features a DoD system using 128 bit RSA, which is broken by one of the actors. What is your reaction to that?

(c) Can encryption and/or decryption of RSA be sped up by the Chinese Remainder Theorem?

(d) Let (N, e) be a public RSA key and d the corresponding private key.

It is commonly stated that $ed \equiv 1 \pmod{(p-1)(q-1)}$, where p, q are the prime factors of N. Give a stronger congruence which actually holds.

(e) Give two examples of side-channels that can be exploited in a side-channel attack.

(f) What is a NOBUS backdoor?

(g) Let p be a large prime. State the discrete logarithm problem, the computational Diffie-Hellman problem as well as the decisional Diffie-Hellman problem, all modulo p. Rank these three problems by their difficulty.

(h) Which primes p are called safe? What is the implication of using a safe prime for ElGamal?

Armin Straub
straub@southalabama.edu

Problem 4.

(a) A hash function $h(x)$ is called one-way if .

(b) A hash function $h(x)$ is called (strongly) collision-resistant if .

(c) Does using a hash function provide authenticity?

(d) What's the difference between a compression function and a hash function? Which construction allows us to create the latter from the former?

(e) Let E_k be encryption using a block cipher (like AES). Is the compression function $\tilde{H}$ defined by

$$\tilde{H}(x,k) = E_k(x)$$

one-way? If it isn't, suggest a variation which is expected to be collision-resistant.

(f) Is SHA-2 considered a secure password hashing algorithm?

(g) What does it mean to salt a password?

(h) In which sense are MD5 and SHA-1 broken? For which purposes must they not be used anymore? For which purposes is it still acceptable to use these hash functions?

(i) Explain why using a hash with, say, 64 output bits is completely inappropriate for digital signatures.

(j) List the main ideas for storing human passwords for authentication.

(k) You need to hash (salted) passwords for storage. Unfortunately, you only have SHA-2 available. What can you do?

(l) We have learned about the birthday paradox. What is its implication for hash functions?

(m) Let H be a cryptographic hash function. What is a simple way to construct a MAC from H?

(n) Both digital signatures and MACs provide authenticity. What aspect of authenticity do digital signatures provide that MACs don't?