Midterm 2 Review

CS 161: Computer Security

Prof. Raluca Ada Popa

April 6, 2020

Announcements

- Starting recording
- Please turn on video if you can
- No discussion sessions this week
- Midterm 2 April 6 at 5pm PT
  - Honor code
  - Randomization, length
  - Exams “encrypted”
  - Encrypted PDFs by 3pm

2016 Midterm 1, Problem 3

Problem 3 ***Good and bad hashes*** **(18 points)**

The following are some hash function candidates h'. For each, circle whether it is collision resistant or a one-way function (could be either, none, or just one). If you do not circle one property (indicating that h' does not satisfy it), give a concrete example of when h' fails, namely, either show how to invert the function or exhibit two values that collide. (And if you do not circle both properties, you should supply a counterexample for each). Assume that h is a secure cryptographic hash function.

h' is one way: There is no poly time attacker that can: for x random, for y = h(x), construct x' s.t. h(x') = y, where x and x' could be different or the same

h' is collision-resistant: No poly time attacker can find any collision h(x) = h'(x) for x and x' different

2016 Midterm 1, Problem 3

Problem 3 ***Good and bad hashes*** **(18 points)**

The following are some hash function candidates h'. For each, circle whether it is collision resistant or a one-way function (could be either, none, or just one). If you do not circle one property (indicating that h' does not satisfy it), give a concrete example of when h' fails, namely, either show how to invert the function or exhibit two values that collide. (And if you do not circle both properties, you should supply a counterexample for each). Assume that h is a secure cryptographic hash function.

(a) ONE WAY or COLLISION RESISTENT: $h'(x) = x$

Not one way (trivial inversion) but CR because no collisions

2016 Midterm 1, Problem 3

Problem 3 ***Good and bad hashes*** **(18 points)**

The following are some hash function candidates h'. For each, circle whether it is collision resistant or a one-way function (could be either, none, or just one). If you do not circle one property (indicating that h' does not satisfy it), give a concrete example of when h' fails, namely, either show how to invert the function or exhibit two values that collide. (And if you do not circle both properties, you should supply a counterexample for each). Assume that h is a secure cryptographic hash function.

(b) ONE WAY or COLLISION RESISTENT: $h'(x) = h(h(x))$

Both

2016 Midterm 1, Problem 3

Problem 3 ***Good and bad hashes*** **(18 points)**

The following are some hash function candidates h'. For each, circle whether it is collision resistant or a one-way function (could be either, none, or just one). If you do not circle one property (indicating that h' does not satisfy it), give a concrete example of when h' fails, namely, either show how to invert the function or exhibit two values that collide. (And if you do not circle both properties, you should supply a counterexample for each). Assume that h is a secure cryptographic hash function.

(c) ONE WAY or COLLISION RESISTENT: h'(x) = h(x) mod 10, where 10 is just the constant number 10

Not one way because you can try a few values and find a preimage, not CR since lots of collisions with only 10 possible hash values

2016 Midterm 1, Problem 3

Problem 3 ***Good and bad hashes*** **(18 points)**

The following are some hash function candidates h'. For each, circle whether it is collision resistant or a one-way function (could be either, none, or just one). If you do not circle one property (indicating that h' does not satisfy it), give a concrete example of when h' fails, namely, either show how to invert the function or exhibit two values that collide. (And if you do not circle both properties, you should supply a counterexample for each). Assume that h is a secure cryptographic hash function.

(d) ONE WAY or COLLISION RESISTENT: h'(x) = h(first $n-1$ bits of x), where n is the number of bits of x

One way, but you can create a collision by changing the last bit

2016 Midterm 1, Problem 3

Problem 3 ***Good and bad hashes*** **(18 points)**

The following are some hash function candidates h'. For each, circle whether it is collision resistant or a one-way function (could be either, none, or just one). If you do not circle one property (indicating that h' does not satisfy it), give a concrete example of when h' fails, namely, either show how to invert the function or exhibit two values that collide. (And if you do not circle both properties, you should supply a counterexample for each). Assume that h is a secure cryptographic hash function.

(e) ONE WAY or COLLISION RESISTENT: h'(x) $= g^x \mod p$ for p a large prime and g a random generator mod p

One way because of discrete log problem, but not CR because x and x + p -1 collide

2016 Midterm 1, Problem 3

Problem 3 ***Good and bad hashes*** **(18 points)**

The following are some hash function candidates h'. For each, circle whether it is collision resistant or a one-way function (could be either, none, or just one). If you do not circle one property (indicating that h' does not satisfy it), give a concrete example of when h' fails, namely, either show how to invert the function or exhibit two values that collide. (And if you do not circle both properties, you should supply a counterexample for each). Assume that h is a secure cryptographic hash function.

(f) ONE WAY or COLLISION RESISTENT: h'(x) = h(x) | "hello", where '|' denotes concatenation

Both one way and CR, not affected by concatenation of a "hello"

2016 Midterm 1, Problem 3

Problem 3 ***Good and bad hashes*** **(18 points)**

The following are some hash function candidates h'. For each, circle whether it is collision resistant or a one-way function (could be either, none, or just one). If you do not circle one property (indicating that h' does not satisfy it), give a concrete example of when h' fails, namely, either show how to invert the function or exhibit two values that collide. (And if you do not circle both properties, you should supply a counterexample for each). Assume that h is a secure cryptographic hash function.

(g) ONE WAY or COLLISION RESISTENT: $h'(x) = x^2$

Not one way because you can take square root and h'(x) = h'(-x)

2016 Midterm 1, Problem 3

Problem 3 ***Good and bad hashes*** **(18 points)**

The following are some hash function candidates h'. For each, circle whether it is collision resistant or a one-way function (could be either, none, or just one). If you do not circle one property (indicating that h' does not satisfy it), give a concrete example of when h' fails, namely, either show how to invert the function or exhibit two values that collide. (And if you do not circle both properties, you should supply a counterexample for each). Assume that h is a secure cryptographic hash function.

(h) ONE WAY or COLLISION RESISTENT: $h'(x) = h(x) \mid x$

Not one way as x is there in the output, but CR due to same x

Problem 5 ***Securing chat*** **(16 points)**

Consider ACME Corporation's secure online messaging protocol, which is as follows. Each user u has a private key SK_u and a public key PK_u. Assume that ACME correctly distributes users' public keys, and attackers did not interfere with this process.

Consider that Alice wants to communicate with Bob. Alice has PK_{Bob}. The protocol is as follows:

1. Alice randomly generates a symmetric key K.
2. Alice encrypts $wrapped\_K = encrypt(PK_{Bob}, K)$.
3. Alice signs $sig = sign(SK_{Alice}, wrapped\_K)$.
4. Alice sends $(wrapped\_K, sig)$ to Bob.
5. Then, when Alice wants to send a message M to Bob, she computes $T = MAC(K, M)$ and sends (M, T).

These are sent through the Internet, and attackers may observe and modify the data.

(a) Bob has PK_{Alice}. When he receives sig, $wrapped\_K$, M, and T, indicate the steps Bob must take to verify that Alice was the one who sent the message M and that it was not modified by an attacker.

1. verify(PK_Alice, wrapped_K, sig)
2. decrypt(SK_Bob, wrapped_K) -> K
3. compute T' = MAC(K,M) and check that T' = T

Problem 5 ***Securing chat*** **(16 points)**

Consider ACME Corporation's secure online messaging protocol, which is as follows. Each user u has a private key SK_u and a public key PK_u. Assume that ACME correctly distributes users' public keys, and attackers did not interfere with this process.

Consider that Alice wants to communicate with Bob. Alice has PK_{Bob}. The protocol is as follows:

1. Alice randomly generates a symmetric key K.
2. Alice encrypts $wrapped\_K = encrypt(PK_{Bob}, K)$.
3. Alice signs $sig = sign(SK_{Alice}, wrapped\_K)$.
4. Alice sends $(wrapped\_K, sig)$ to Bob.
5. Then, when Alice wants to send a message M to Bob, she computes $T = MAC(K, M)$ and sends (M, T).

(b) Can Alice initiate a conversation with Bob and send him a message while he is offline? Namely, can he verify the message without interacting with Alice?

yes

Problem 5 ***Securing chat*** **(16 points)**

Consider ACME Corporation's secure online messaging protocol, which is as follows. Each user u has a private key SK_u and a public key PK_u. Assume that ACME correctly distributes users' public keys, and attackers did not interfere with this process.

Consider that Alice wants to communicate with Bob. Alice has PK_{Bob}. The protocol is as follows:

1. Alice randomly generates a symmetric key K.
2. Alice encrypts $wrapped\_K = encrypt(PK_{Bob}, K)$.
3. Alice signs $sig = sign(SK_{Alice}, wrapped\_K)$.
4. Alice sends $(wrapped\_K, sig)$ to Bob.
5. Then, when Alice wants to send a message M to Bob, she computes $T = MAC(K, M)$ and sends (M, T).

These are sent through the Internet, and attackers may observe and modify the data.

(c) Bob wants to report that Alice sent messages which violates ACME's rules. He decides to disclose the transcript (containing sig, $wrapped\_K$, M, and T) and K to Charlie, who works at ACME. Charlie also has PK_{Alice}. Does this information prove that Alice intentionally sent M? If so, how can Charlie verify that? If not, explain why.

No because Bob can create a new MAC for a separate messages.
He has the secret key K for that.

2019 Midterm 2

(c) Which of these URIs have the same origin as "`http://same.origin.com:80/a.htm`" according to same origin policy? (choose 0 to 4 options)

- [ ] `http://origin.com:80/a.htm`
- [ ] `http://same.origin.com:80`
- [ ] `http://same.origin.com:80/a.htm/b`
- [ ] `ftp://same.origin.com:80`

(d) If a page loads a JavaScript file from some other site, this JavaScript file takes the origin of...

Choose one option:

- [ ] The page that loaded it
- [ ] The site that hosts the JavaScript file

(e) Same-origin policy is very useful in preventing many web attacks. Yet, it also inconveniences for web developers – different domains cannot talk to each other.

◇ **Question:** Provide a *specific* solution for the web developers to *conveniently* enable JavaScript in different domains' webpages to *conveniently* talk to each other. (answer less than 10 words)

postMessage – narrow API

Good luck on the midterm!