Tech Notes

Tuesday, January 24, 2017

Week 2 Quiz

1. Two ASCII messages containing English letters and spaces only are encrypted using the one-time pad and the same key. The 10th byte of the first ciphertext is observed to be 0xB7 and the 10th byte of the second ciphertext is observed to be 0xE7. Let m1 (resp., m2) denote the 10th ASCII character in the first (resp., second) message. What is the most you can conclude about m1 and m2?

One of m1 or m2 is the space character, and the other is the character 'p'.
m1 is the space character and m2 is the character 'p'.
m1 is the character 'p' and m2 is the space character.
m1 is the character 'B' and m2 is the character 'E'.
Nothing can be determined about m1 or m2 since the one-time pad is perfectly secret.

2. Three ASCII messages containing English letters and spaces only are encrypted using the one-time pad and the same key. The 10th byte of the first ciphertext is observed to be 0x66, the 10th byte of the second ciphertext is observed to be 0x32, and the 10th byte of the third ciphertext is observed to be 0x23. Let m1 (resp., m2, m3) denote the 10th ASCII character in the first (resp., second, third) message. What is the most you can conclude about m1, m2, and m3?

Nothing can be determined about m1, m2, or m3 since the one-time pad is perfectly secret.
m1 is the character 't', m2 is the space character, and m3 is the character 's'.
m1 is the space character, m2 is the character 't', and m3 is the character 'e'.
Exactly one of m1, m2, or m3 is the space character, but nothing else can be determined.

3. Which of the following is true about computational secrecy? (Select all that apply.)

Computational secrecy means that it is trivial for an attacker to always learn the entire message.
Computational secrecy currently relies on unproven assumptions.
Computational secrecy only ensures secrecy against attackers running in some bounded amount of time.
Computational secrecy allows an attacker to learn information about the message with small probability.

4. Let G be a function mapping n-bit inputs to 2n-bit outputs. Which of the following is true of the pseudo one-time pad encryption scheme based on G? (Check all that apply.)

The scheme is computationally secret if G is a pseudorandom generator.
The key space of the scheme is at least as large as the message space.

Pages

- OSCP (Offensive Security Professional)

Search This Blog

Search

Blog Archive

▼ 2017 (13)
► May (8)
▼ January (5)
Software Security Quiz 1
Hardware Quiz 2
Hardware Quiz 1
Week 2 Quiz
Cryptography Quiz 1

The scheme can be used securely to encrypt multiple messages using the same key.
The scheme is perfectly secret.

5. Which of the following attackers can be used to demonstrate that the shift cipher for 3-character messages does not satisfy perfect indistinguishability?

Output m0 = 'aaa' and m1 = 'abc'. Given challenge ciphertext C, output 0 if the first character of C is 'a'.
Output m0 = 'aaa' and m1 = 'bbb'. Given challenge ciphertext C, output 0 if the first character of C is 'a'.
Output m0 = 'aaa' and m1 = 'abc'. Given challenge ciphertext C, output 1 if the three characters of C are all different.
Output m0 = 'abc' and m1 = 'bcd'. Given challenge ciphertext C, output 1 if the three characters of C are all different.

6. Which of the following is a negligible function? (Check all that apply.)

f(n) = 1/n.
f(n) = 1/2^n
f(n) = 1/2
f(n) = n/2^n

7. Define the following function G taking n-bit inputs and producing (n+1)-bit outputs: G(x)=x‖0, where ‖ denotes concatenation. Which of the following attackers shows that this G is not a pseudorandom function?

On input an (n+1)-bit string y, output 0 if the last bit of y is 0.

On input an (n+1)-bit string y, output 1 if the first bit of y is 0.

On input an (n+1)-bit string y, output 0 if the first bit of y is 0.

On input an (n+1)-bit string y, output 0 if the first bit of y is equal to the last bit of y.

8. Say G is a pseudorandom generator taking n-bit inputs and producing 2n-bit outputs. Which of the following are necessarily true? (Check all that apply. The symbol '|' is used here for string concatenation.)

G(r) | G(r+1) is computationally indistinguishable from a uniform, 4n-bit string if r is a uniform n-bit string.

G(r) is computationally indistinguishable from a uniform, 2n-bit string if r is a uniform n-bit string.
r | G(r) is computationally indistinguishable from a uniform, 3n-bit string if r is a uniform n-bit string.
G(0 | r) is computationally indistinguishable from a uniform, 2n-bit string if r is a uniform (n-1)-bit string.

9. Which of the following is a setting in which a pseudorandom generator could be applied?

You have a 1 MB file that you would like to compress.
You have a way to generate random bits at the rate of 100 bits/second, but you need 1,000,000 random bits to run a statistical simulation.
You have a 1 MB file and you would like to make sure that it has not been tampered with.

10. Consider a pseudo one-time pad encryption scheme Π constructed using some function G. Which of the following did our proof of security for the pseudo one-time pad show?

Π is always perfectly secret, for any G.
If G is a pseudorandom generator, then Π is computationally secret.
If G is a pseudorandom generator, then Π is perfectly secret.
Π is always computationally secret, for any G.

Posted by Ck at 9:13 PM

5 comments:

sandeep saxena June 13, 2019 at 4:58 AM

I am feeling happy to read this. You gave nice info to me. Please update more.
Hibernate Training in Chennai
Spring Hibernate Training in Chennai
Hibernate Training in Velachery
Spring Training in Chennai
Spring framework Training in Chennai
Struts Training in Chennai
Wordpress Training in Chennai

Reply

Replies

Unknown October 6, 2020 at 12:47 PM

IEEE Final Year Project centers make amazing deep learning final year projects ideas for final year students Final Year Projects for CSE to training and develop their deep learning experience and talents.

IEEE Final Year projects Project Centers in India are consistently sought after. Final Year Students Projects take a shot at them to improve their aptitudes, while specialists like the enjoyment in interfering with innovation.

corporate training in chennai corporate training in chennai

corporate training companies in india corporate training companies in india

corporate training companies in chennai corporate training companies in chennai

I have read your blog its very attractive and impressive. I like it your blog.
Digital Marketing Company in Chennai

Reply

punitha June 16, 2019 at 11:21 PM

Remarkable post! That's a lot of information. Thanks for taking your time and effort to share this with us. Keep us updated.
Blue Prism Training in Chennai
Blue Prism Training Institute in Chennai
AWS Training in Chennai
Cloud Computing Training in Chennai
Data Science Course in Chennai
RPA Training in Chennai
VMware Training in Chennai

Reply

sheela rajesh June 17, 2019 at 3:50 AM

Really nice blog,i enjoyed your infomations. Thank you and i will expect more in future.
JAVA Training in Chennai
JAVA Course in Chennai

Big data training in chennai
Software testing training in chennai
Selenium Training in Chennai
Python Training in Chennai
JAVA Training in Tambaram

Reply

sangeetha sathyan July 13, 2019 at 4:57 AM

I wanted to thank for sharing this article and I have bookmarked this page to check out new stuff.
Tally course in Chennai
Tally classes in Chennai
Tally Training in Chennai
ccna course in Chennai
PHP Training in Chennai
Salesforce Training in Chennai
Web Designing course in Chennai
Tally Course in Porur
Tally Course in OMR
Tally Course in Tambaram

Reply

Enter your comment...

Comment as: Google Account

Publish Preview

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)