CS 490: Cryptography and Computer Security

Homework #01

Assigned Date	: Thursday, January 29, 2015
Due Date	: Thursday, February 12, 2015 @ 09:29:59 a.m.

Instructions

- This is an individual assignment. **Do your own work**. Acts of academic misconduct (plagiarism, use of illicit solutions manuals, etc.) are subjected to university code of conduct.
- Produce your answers using an appropriate word processing application.
- Submit your solutions through Moodle. A dropbox will be available with 24 hours in advance of the deadline. Late policy is enforced per syllabus late policy. Your digital submission must be in PDF format. Grades and specific feedback will be communicated through Moodle.
    - You may, **in addition** to the digital submission, handover a printed, stapled copy of your answers to the instructor at the beginning of class, **if** you prefer to have explicit written feedback of your answers. This, however, is not required neither is considered the primary submission option.
- **DO NOT** email your solutions to the instructor.
- Make proper arrangements, after consulting the instructor, to deliver your solutions **BEFORE** the due date, if you have a planned absence on the due date.
- Answer all questions
- Your solutions are due on **Thursday, February 12, 2015 @ 09:29:59 a.m.**
- Total points: **[UG: 200, MS: 350 points]**

Questions

Q1. [**35 points**] Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

Q1.a [**5 points**] Jim copies Mary's homework.

Q1.b [**5 points**] Pete crashes Linda's system.

Q1.c [**5 points**] Carol changes the amount of Angelo's check from $100 to $1000.

Q1.d [**5 points**] Gina forges Roger's signature on a deed.

Q1.e [**5 points**] Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.

Q1.f [**5 points**] Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.

Q1.g [**5 points**] Henry spoofs Julie's IP address to gain access to her computer.

Q2. [**30 points**] What security service(s) are guaranteed when using each of the followin methods to send mail at the post office?

Q2.a [**5 points**] Regular mail.
Q2.b [**5 points**] Regular mail with delivery confirmation.
Q2.c [**5 points**] Regular mail with delivery and recipient signature.
Q2.d [**5 points**] Certified mail.
Q2.e [**5 points**] Insured mail.
Q2.f [**5 points**] Registered mail.

Q3. [**15 points**] Define the type of attack in each of the following cases:

Q3.a [**5 points**] Henry breaks into Dr. Gamage's office to obtain the solution guide of PR01.
Q3.b [**5 points**] Carol gives a check for $10 to buy a used book. Later she finds that the check was cached for $100.
Q3.c [**5 points**] Pete sends hundreds of e-mails per day to Malinda using a phony return e-mail address.

Q4. [**20 points**] Distinguish between Z, Z_n, and Z_{n^*}. In which set does each element have an additive inverse? In which set does each set have an multiplicative inverse? Which algorithm is used to find the multiplicative inverse of an integer in Z_n?

Q5. [**15 points**] A small private club has only 100 members. Answer the following questions.

Q5.a [**5 points**] How many secret keys are needed if all members of the club need to send secret messages to each other?
Q5.b [**5 points**] How many keys needed if everyone trusts the president of the club, and routes communication through him when they need to talk with each other.
Q5.c [**5 points**] How many keys needed if the president decides to create temporary session keys for the two parties needing to communicate. The temporary key is encrypted and sent to both members.

Q6. [**15 points**] Suppose that spaces, periods, and question marks are added to the plaintext to increase the key domain of simple ciphers. What is the key domain if:

Q6.a [**5 points**] an additive cipher is used?
Q6.b [**5 points**] a multiplicative cipher is used?
Q6.c [**5 points**] an affaine cipher is used?

Q7. [**15 points**] Suppose Alice and Bob decided to ignore Kerckhoff's principle and hide the type of the cipher they are using.

Q7.a [**5 points**] How can Eve decide whether a substitution cipher or a transposition cipher was used?
Q7.b [**5 points**] If Eve knows that a substitution cipher is used, how can she decide whether it is additive, multiplicative, or affaine?
Q7.c [**5 points**] If Eve knows that transposition cipher is used, how can she find the size of the section/period?

Q8. [**15 points**] Encrypt the message "this is an example" using one of the following ciphers. Ignore the spaces between words. Decrypt the message to get the original plaintext. Show your work.

Q8.a [**5 points**] Additive cipher with key $= 20$
Q8.b [**5 points**] Multiplicative cipher with key $= 15$

Q8.c [**5 points**] Affaine cipher with key = (15,20)

Q9. [**10 points**] Encrypt the message “the house is being sold tonight” using Vigenere cipher. Ignore the spaces between words. Decrypt the message to get the original plaintext. Show your work.

Extra Credit

Q10. [**15 points**] Write a program to achieve the objectives of Q8. Submit your properly documented code with compilation and run instructions.

Q11. [**15 points**] Write a program to achieve the objectives of Q9. Submit your properly documented code with compilation and run instructions.

MS Requirements

Q12. [**150 points**] Prepare a summary critique (between 3/4 - 1 page, single space, PDF format) for each of the graduate readings assigned to you on 01/20/2014. Formulate each critique based on your answers for the following questions.

(a) Title, author(s), date of publication, and venue
(b) What is the primary contribution(s) (according to the authors) of this paper?
(c) What are the critical assumptions (if any) of this paper?
(d) Justify the applicability (or inapplicability) and the validity (or invalidity) of the original contributions to present day networking. *You must logically justify your arguments*.
(e) Propose at least 2 additional, preferably recent, (*within the last 8-10 years*) publications that a would be reader of this paper must read next.
(f) What is your impression of the primary contribution of this paper?

Graduate Grading

- [**25 × 3 points**] Submit your critiques (3 individual PDFs) through the **HW01: Graduate Critique** forum in Moodle.
- [**25 × 3 points**] Select three critiques, preferably from three different colleagues, and *critique their paper critiques*. Post your comments as replies.