Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout **??**
October 10, 2002

Quiz 1

- **DO NOT OPEN** this quiz until instructed to do so.
- You should not have more than one empty chair between you and the next person. If seating availability permits, do not sit directly next to another person.
- This quiz is **open book**. You may use any of the results presented in class, in the handouts, or in the problem sets.
- There are fifteen (15) problems totaling 100 points. Problems are labelled with their point values.
- Put your name on the top of **every** page – *these pages may be separated for grading.*
- Write your solutions in the space provided. Should you need extra space, write on the back of the sheet containing the question.
- **Be neat and write legibly**. You will be graded not only on the correctness of your answer, but also on the clarity with which you express it.

Problem Q1-1. [4 pts]

Fill in your name and the names of the people sitting next to you. If you are at the end of a row, write $\perp$ in the space provided.

Your name:	
Name of person to your right:	
Name of person to your left:	

DO NOT WRITE ON THIS PAGE

Problem	Grade	Points
Q1-1		4
Q1-2		4
Q1-3		4
Q1-4		7
Q1-5		12
Q1-6		14
Q1-7		5
Q1-8		4
Q1-9		5
Q1-10		3
Q1-11		7
Q1-12		13
Q1-13		6
Q1-14		4
Q1-15		8
Total		100

Problem Q1-2. [**4 pts**]

For a parallel computer (which can do many operations simultaneously) programmed to perform CBC mode encryption (circle the correct answer):

1 Encryption is faster than decryption.

2 Decryption is faster than encryption.

3 Encryption and decryption should run in approximately the same time.

Problem Q1-3. [**4 pts**]

Circle true or false for the following statements. If $\mathcal{P} = \mathcal{NP}$, then:

True **False** The one-time pad still provides information-theoretically secure message authentication.

True **False** Secure encryption becomes impossible.

True **False** Shamir's secret-sharing technique becomes insecure.

True **False** One-way functions do not exist.

Problem Q1-4. [7 pts]

Circle true or false for the following statements:

True **False** Alma Whitten's experiments show that PGP 5.0's graphical user interface is not sufficiently effective to provide security for most users.

True **False** The WSJ cookie authentication scheme was insecure because of sequential session IDs.

True **False** A cryptographically secure hash function $h : \Sigma^* \to \Sigma^k$ (OW, CR) must be injective.

True **False** Triple-DES uses uses three unique 56-bit DES keys.

True **False** Consecutive Fibonacci numbers are the worst-case input for Euclid's Algorithm.

True **False** The El Gamal encryption scheme is plaintext-aware.

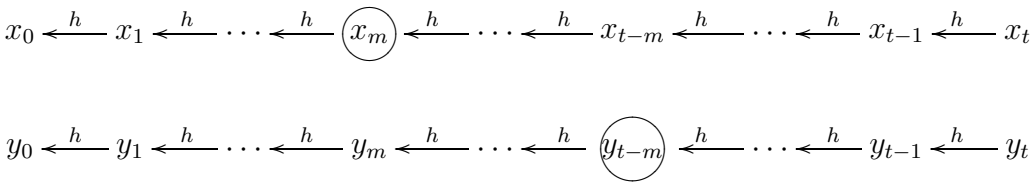
True **False** To make a deterministic public-key encryption scheme secure against an adaptive chosen ciphertext attack, it suffices to pad the given plaintext with some random bits before encryption (such random bits being discarded upon decryption).

Problem Q1-5. [12 pts]

Consider the following generalization of Lamport's one-time signature scheme, for signing a value m, where m is drawn from a finite set $\{1, 2, \ldots, t\}$ for some $t > 2$.

The use-once portion of the key used to sign m consists of two values x_0 and y_0. Here x_0 and y_0 are the roots of hash chains of length $t + 1$. That is, $x_i = h(x_{i+1})$ for $0 \leq i < t$ and $y_i = h(y_{i+1})$ for $0 \leq i < t$, where h is a one-way hash function.

To sign m, where $1 \leq m \leq t$, the signer reveals both $X = x_m$ and $Y = y_{t-m}$. The signature can be verified by checking that $h^m(X) = x_0$ and $h^{t-m}(Y) = y_0$.



(a) [6 pts]

Why are two chains used per value signed? (Why not eliminate the y chain?)

(b) [6 pts]

Argue briefly that this scheme is secure, if h is indeed one-way. (Why can't a forger produce a signature for a different value m', after having seen the signature for m?)

Problem Q1-6. [14 pts]

(a) [4 pts]

Recall that the WSJ used crypt() in its MAC, MAC_k = crypt(username||secret) where || denotes concatenation. Assume that the secret can be any sequence of 8-bit (not necessarily printable) characters. Give the maximum number of Web queries an interrogative adversary must make to achieve a total break (universal forgery).

(b) [4 pts]

The Backstreet Journal, a new branch of the WSJ catering to aging pop-star financial news, decided to use a cryptographically secure (OW, CR) hash function $h : \{0, \ldots, 255\}^k \to \{0, \ldots, 255\}^{20}$ instead of crypt() in MAC_k. Similar to crypt(), the h function truncates input after the kth byte. Give the maximum number of Web queries an interrogative adversary must make to achieve a total break (universal forgery) if the secret is any sequence of 8-bit (not necessarily printable) characters. You can assume that usernames can be any length.

(c) [6 pts]

If the WSJ had used SHA-1 instead of crypt() in its MAC, would you expect the scheme to be stronger? Why or why not?

Problem Q1-7. [5 pts]

For each of the following applications, list the necessary hash function properties (OW, CR, WCR):

PGP fingerprints	
Unix password files	
Secure URLs	
Hash cash	
One-time passwords	

Problem Q1-8. [4 pts]

Ben Bitdiddle upgraded his plaintext telnet server to a telnet server with one-time passwords based on the Lamport password authentication scheme. Which of the following attacks is Ben's new system no longer or less susceptible to (circle all that apply):

1 Replay attack

2 Session hijacking

3 Dictionary attack on stolen database

4 Keystroke logging

Problem Q1-9. [5 pts]

In the list below, circle the symmetric block ciphers:

AES	DES	DSA/DSS	El Gamal	RC4
RC5	RC Cola	Rijndael	RSA	Triple-CBC

Problem Q1-10. [3 pts]

Name one cipher from previous question that is a Feistel cipher:

Problem Q1-11. [7 pts]

In the Digitarian World, people don't have names, but numbers to identity themselves. A group of four students (12, 25, 20, 5) attending the university 13-9-20 is taking 6.857. They are having some issues trying to do problem set 3 problem 1: they just can't find a large prime p such that all their numbers are generators of $\mathcal{Z}_p^*$.

Explain briefly why they could not succeed.

Problem Q1-12. [13 pts]

Let p be a prime, and $g \in \mathcal{Z}_p^*$ be an element of order q, where q is a prime ≥ 3 (note that g is *not* a generator of $\mathcal{Z}_p^*$).

(a) **[5 pts]** What are valid formulas for the inverse of g modulo p? Circle all correct answer(s).

$g^{q-1} \bmod p$ $\quad$ $g^{q} \bmod p$ $\quad$ $g^{p-2} \bmod p$ $\quad$ $g^{p-1} \bmod p$ $\quad$ $g^{p} \bmod p$

$g^{q-1} \bmod q$ $\quad$ $g^{q} \bmod q$ $\quad$ $g^{p-2} \bmod q$ $\quad$ $g^{p-1} \bmod q$ $\quad$ $g^{p} \bmod q$

(b) **[4 pts]** Give a formula for the square root of g modulo p.

(c) **[4 pts]**

For an integer $e \geq 3$ such that $gcd(e, q) = 1$, explain briefly how to compute the e^{th} root of g modulo p, *i.e.* find an h such that $h^e = g \pmod p$.

Hint: You may find some inspiration by looking at the RSA encryption/decryption process.

Problem Q1-13. [6 pts]

In the RSA scheme, the modulus $n = pq$ is chosen as a product of two large primes $p < q$. To make factoring n as hard as possible, Ben Bitdiddle decides to make the smaller prime p as large as possible, and thus chooses p and q as consecutive primes.

Explain briefly why Ben's approach is flawed. You can assume that p and q are reasonably close to each other.

Problem Q1-14. [4 pts]

Ben Bitdiddle is using Shamir's (k, n) threshold secret sharing scheme, where n persons want to share a secret of N-bits, so that the shares of k persons are needed to reveal the secret. Ben chooses the prime p to be $(N + 1)$-bits.

What is the approximate size (in bits) of each person's share? Circle the correct answer:

$N\frac{1}{k}$ $N\frac{1}{n}$ $N\frac{k}{n}$ $N\frac{n}{k}$ N

Problem Q1-15. [**8 pts**]

Figure 1: Plaintext picture.

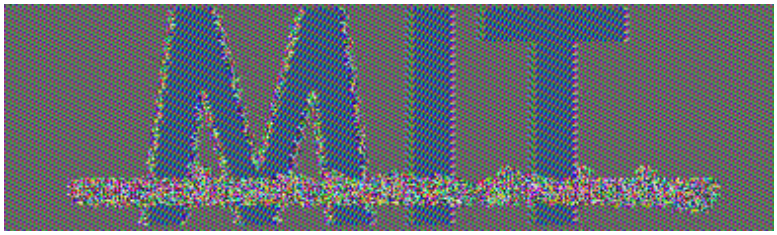


Figure 2: Encrypted picture.

Figure **??** is an encrypted version of Figure **??**. The picture was encrypted with DES. The graphic format is very simple. It consists of a sequence of RGB values (ranging from 0 to 255). Each pixel takes three bytes (one for each color). The dimensions of the graphic is known a priori (390×115 pixels). In the binary file, the $(3(x + 390y))$th byte denotes the red color of the pixel at location (x, y). A similar formula describes the location of the green and blue colors of pixels. What block cipher block mode did we use to encrypt this graphic?

Explain your reasoning.