DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

6.033—Computer System Engineering　　　　Handout 23—April 11, 1996

Quiz 2 Sample Questions

Here is the FAA (Frequently Answered Answers) for Quiz 2:

1. Quiz 2 will be from 2-3pm on Friday, April 19, 1996.

2. There are ***three*** rooms. Go to the room that corresponds to your last name:

4-270	<--->	A to H
4-370	<--->	I to R
2-190	<--->	S to Z

3. The quiz will cover all the material from R8 (recitation 8) to R16. That's from March 5 to April 9.

4. There will be a quiz review from 7-9pm on Wed. April 17 in 34-101.

5. Yes, the quiz is open-book, open-notes.

Below are the quizzes from the previous two years. Solutions to these questions will be handed out next week so you can have some time to work on the questions on your own. Have fun and good luck.

Oh, and in case you need this but don't know what the Web is (haha), here are the official TA hours:

Dawson Engler	R11-1	NE43-520
Jack Fu	M1-2, R12-1	24-321
Eddie Kohler	M12-1, R3-4	NE43-521a
Ulana Legedza	F3-4, M4-5	NE43-536
Jonathan Litt	M4-5, R4-5	24-321
Yoav Yerushalmi	M4-5:30	24-323

Spring 1994 Quiz 2

Problem 1. *(25 points)* Lucifer is determined to figure out Alice's password by a brute-force attack. From watching her log in he knows that her password is eight characters long and all lower-case letters. He sets out to try all possible combinations of eight lower-case letters.

a. Assuming he has to try about half the possibilities before he runs across the right one, one trial can be done in one machine cycle, and he has a 60 MHz computer available, about how long will the project take?

b. How long will it take if Alice chooses an eight-character password that includes upper- and lower-case letters, numbers, and special characters? There are 78 characters available for her to choose from.

c. Suppose processors continue to get faster, improving by a factor of three every two years. How long will it be until Alice's new password can be cracked as easily as her old one?

Problem 2. *(24 points)* Louis Reasoner is fascinated with the discovery that some encryption algorithms are *commutative*.

For this problem we use the usual notation: A message M that is encrypted with key k is written $\{M\}^{k}$. A commutative scheme has the interesting property that for every message and every pair of keys k1 and k2, $\{\{M\}^{k1}\}^{k2} = \{\{M\}^{k2}\}^{k1}$. That is, you get the same result no matter which order two encryptions with different keys are done.

Louis has proposed that Alice, in San Francisco, and Bob, in Boston, use the following scheme for secure delivery of messages between their computers, which are connected via the Internet:

Alice chooses a never-before-used (nonce) encryption key, Ka, encrypts her message M, and sends the result, $\{M\}^{Ka}$, to Bob. Bob chooses another nonce encryption key, Kb, encrypts the already-encrypted message to produce $\{\{M\}^{Ka}\}^{Kb}$ and sends the doubly-encrypted result back to Alice. By commutativity, this message is identical to $\{\{M\}^{Kb}\}^{Ka}$, which is a message that Alice can decrypt with her nonce Ka. She does so, revealing $\{M\}^{Kb}$. This result she sends back to Bob, who can now decrypt it with his nonce Kb to reveal M.

The appealing thing about this scheme is that Alice and Bob did not have to agree on a secret key in advance. Louis calls this the "No-Prior-Agreement" protocol.

a. Is it possible for a passive intruder (that is, one who just listens to the encrypted messages) to discover M? If so, describe how. If not, explain why not.

b. Is it possible for an active intruder (that is, one who can also insert, delete, or replay messages) to discover M? If so, describe how. If not, explain why not.

Problem 3. *(10 points)* One way of speeding up a name resolution system is to implement a cache that remembers recently looked-up {name, object} pairs. *Synonyms* are multiple names for the same object. What problems do synonyms pose for cache designers?

Problem 4. *(15 points)* Alyssa is trying to organize her notes on virtual memory systems, and it occurred to her that virtual memory systems can usefully be analyzed as naming systems. She has gone through her 6.033 notes and made a numbered list of some technical terms from the lectures on naming systems; that list is on the right, below. She then listed some mechanisms found in virtual memory systems on the left. But she isn't sure which naming concept goes with which mechanism. Help Alyssa out by placing in each blank on the left the number of the term on the right that best applies to this mechanism. Hint: no number needs to be used twice.

	1. Search path
_____a. page map	2. Naming network
_____b. virtual address	3. Closure
_____c. physical address	4. Object
_____d. a TLB entry	5. Name
_____e. the processor register that points to the page map	6. Context
	7. None of the above

Problem 5. *(25 points)* The network level of the Internet names hosts with 4-byte *host addresses*. These names are assigned regionally, with all hosts in one major region receiving host addresses for which the first byte is the same. A region is divided into sub-regions in which all host addresses have the same value for the second byte, and so on. This hierarchical naming scheme is used by the routing system to reduce the size of the tables it must maintain.

a. Explain briefly how hierarchical naming of host addresses might reduce the size of routing tables.

b. Ben Bitdiddle is thinking about designing a system for wireless attachment of portable computers to the Internet. He has decided that the basic architecture should consist of a number of fixed base stations, each of which will communicate by radio with those portable computers in its area. He plans to make each base station a sub-sub-region, using the third byte of the Internet address to identify it. Alyssa points out that this plan limits the number of portables that can simultaneously work with one base station. The base station uses up one of the host addresses for its sub-sub-region. How many portables can work with one base station?

c. Ben proposes not to permanently assign host addresses to portable computers. Instead, when a portable is switched on, it will ask some base station to dynamically assign a host address for it to use. When dynamic address assignment is used, what else has to happen in order for other computers to initiate communication with a portable?

d. Ben wants his design to work with the portable computer mounted on the handlebars of his bicycle. The base stations he will use were designed for cellular phones, so they have the ability at the physical transport level to transfer (or "handoff") a conversation from one base station to another as the signal strength changes. But in Ben's design a handoff means that the host address of the portable must change. Ben wants to be able to maintain connections through handoffs, so that he can transfer long files without disruption while cycling across town. His first idea is to modify the File Transfer Protocol to allow handoff. Whether or not he figures out how to do the modification, what is the main defect in this proposal?

e. ***Briefly*** suggest a way of accomplishing handoff entirely within the network layer.

Extra Problems

Problem 2 (16 points)

The report "Computers at Risk" and the readings on the Internet Worm show that each of the following entities can take actions which will improve the security of computer systems that are attached to the Internet. For each of the entities listed below, give one distinct action in one short sentence. (Don't use the same action for different entities.)

(a: 4 pts) The individual user.

(b: 4 pts) The system administrator.

(c: 4 pts) The seller of operating system software.

(d: 4 pts) The Information Security Foundation, whose establishment is a principal recommendation of "Computers at Risk".

Problem 4: Authentication (21 points)

Consider the following Kerberos-like protocol.

ticket ::= $\{A, B, t_{ticket}, K_C\}^{K}{}_{B}$

auth ::= $\{A, t_{auth}\}^{K}{}_{C}$

tx ::= x's timestamp

1. *A -> KDC: A, B*
2. *KDC -> A:* $\{K_C, t_{ticket}, ticket\}^{K}{}_{A}$
3. *A -> B: {auth}, {ticket}*
4. *B -> A:* $\{t_{auth} + 1\}^{K}{}_{C}$

(a: 4 pts) What does the last message accomplish?

B decrypts the ticket sent in line 3 and observes that A wants to initiate a conversation with B using K_C.

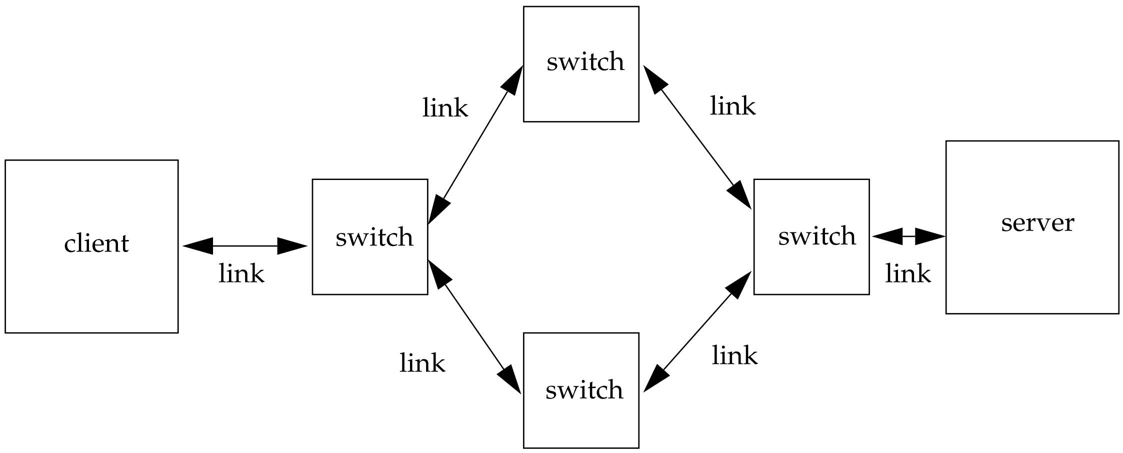
(b: 8 pts) What else can B deduce concerning the ticket itself? Explain briefly.

(c: 4 pts) What else can B deduce concerning A? Explain briefly.

(d: 5 pts) Ben Bitdiddle insists that sending {*auth*} in line 3 is redundant. He proposes changing line 3 to A -> B: {*ticket*}. What are the implications of this change on the protocol?

Section 3: More networks (18 pts)

Consider the following network, in which the client wants to transfer files to and from the server. For the purposes of this section, communication is considered *reliable* when packets are transferred without errors, in order, and without loss.



A. (9 pts) Assume for this part that communication over a link is reliable. Must the client and server worry about the reliability of their file transfer? Explain briefly.

B. (9 pts) Now suppose that the links do not provide reliable communication. The client and the server use end-to-end techniques to ensure reliability. Briefly explain the tradeoff involved in making the links more reliable.

7A.9

Ben Bitdiddle has been using the following protocol for distributing conversation keys, with a private-key server:

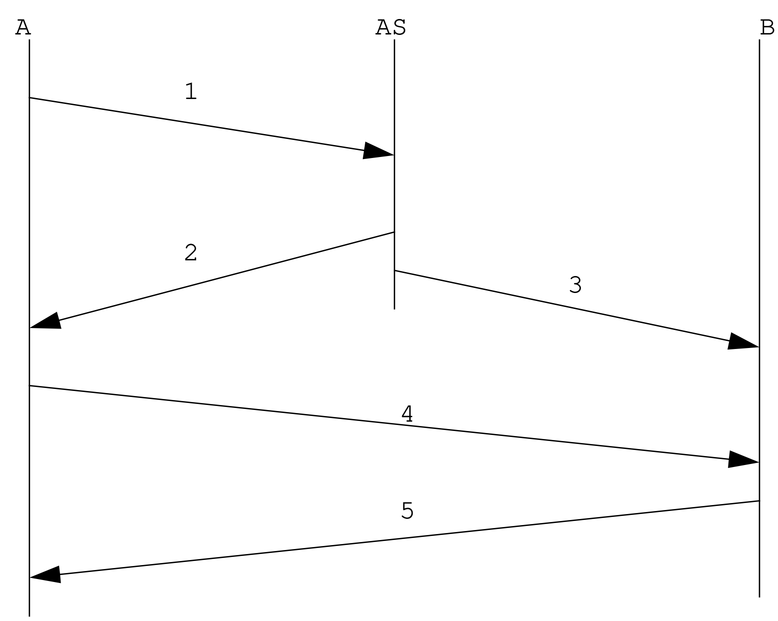
1. A -> AS: $\{A, B, I_a\}$
2. AS -> A: $\{B, I_a, C_k\}K_a$
3. AS -> B: $\{A, I_a, C_k\}K_b$

where A is initiating a communication with B, and I_a is a nonce identifier chosen by A to distinguish this communication from all others its has ever carried on with B. Every time Authentication Server AS is invoked, it issues a new, random key, C_k.

Once the keys are distributed, A and B complete the communication as follows:

4. A -> B: $\{Question\}C_k$
5. B -> A: $\{Answer, I_a\}C_k$

where "Question" is a 16-bit integer that B uses as an index into a table of 65536 entries to find "Answer." When A receives "Answer" it verifies that this is the answer to "Question" by checking that the returned Ia is the original nonce. Now the communication is complete and A and B discard key C_k. If A makes another inquiry of B, A obtains another key first. The key distribution protocol and the ensuing completed communication are illustrated in the following time diagram:



Ben has noticed that the network has become unreliable lately, so he is trying to add a timeout-retry algorithm to make this protocol more reliable. He has one important constraint: the authentication server was audited, certified, and padlocked last summer, so Ben is not allowed to change its program.

(continued on the next page)

Ben has come up with the following retry protocol:

i. `A` sends message 1 and sets a timer. If the timer goes off before message 2 arrives, `A` chooses a new nonce and sends a new message 1. `A` repeats this activity until a message 2 returns that contains the nonce of the most recently sent message 1. `A` then sends message 4 repeatedly to `B` until a response 5 comes back.

ii. Whenever a message 3 arrives at `B`, `B` stores it in a FIFO queue for `A`. Whenever a message 4 arrives, `B` takes the first message 3 from the FIFO queue and uses its key and nonce to decipher and respond. If the FIFO queue is empty, `B` ignores the message 4 by discarding it.

Ben desperately needs your help in debugging this protocol.

A) Ben tried the protocol a few times and it seemed to work. But the next time he tried it A went into an endless loop. Find the scenario with only one lost message that leads this protocol to enter an endless loop.

B) Ben also notices that sometimes a message 5 returns that seems to contain a nonce different from any that A has ever issued. He calls this event the "mysterious nonce problem". How can this event happen?

C) Haphazard Harry suggests that when either the mysterious nonce problem occurs or A notices it has retried message 4 too many times, the thing for A to do is restart the protocol from the beginning. Upon implementing this change, Ben discovers that even if no more messages are ever lost, the protocol retries forever without succeeding. Why?

D) Cautious Marie likes Haphazard Harry's protocol, but with one minor variation. She suggests that Ben should reprogram A to discard any message 5 that has a mysterious nonce and retry message 4, rather than restarting the protocol. Then, following Harry's idea, when A notices that it has retried message 4 too many times, it should restart the protocol from the beginning. Ben, at wit's end, tries this suggestion and is amazed to find that the protocol now always, eventually, succeeds. Why does Marie's suggestion work?

E) Marie, less cautious now, suggests a simplification: when A retries message 1, she claims there is no need to change the nonce. Is this observation correct? Why or why not?

Section 5: RPC (11 pts)

A. (5 pts) Some commercial RPC packages allow programmers to explicitly declare an exported procedure as *idempotent*. Explain how this permits a simpler RPC implementation over an unreliable communication channel.

B. (6 pts) Give two differences between local procedure calls and RPCs that are visible to programmers.

5.20

Below is a set of concepts relating to naming and binding. After that is a set of examples concerning books and library systems. In the blank to the left of each example, place the letter of the concept that most closely associates with or describes that example. Every concept is used *exactly once*.

For this problem, assume that the call number that is associated with a book has 3 components: the *class number*, the *book number*, and the *publication date*. For example, Wessel's book "Freedom's Edge" is associated with the call number QA76.W47.1974, where "QA76" indicates that the book falls into the "Computer Science and Engineering" category. The remainder of the call number ".W47.1974", ensures that the number is not assigned to any other book in the library.

Concepts

(a) unique identifier
(b) multiple contexts
(c) closure
(d) search rule
(e) containment by copy
(f) containment by name
(g) implied context
(h) name conflict
(i) stable binding

Examples

1. ____ We seldom change the call number that has been assigned to a book.
2. ____ *SIGH* Here is yet another book entitled "An Introduction to Systems Design."
3. ____ The book "Freedom's Edge" can be found in the Student Center LIbrary, as well as the Barker Library.
4. ____ That's interesting. The book "Freedom's Edge" has a different call number at Stanford.
5. ____ If you know the name of the author, use the Author Card Catalog. If not, try the Title Card Catalog, or the Subject Card Catalog.
6. ____ QA76.W47.1974
7. ____ Hmm, this 6.033 handout mentions a book by the name of "An Introduction to Systems Design," It must be the one on Computer Systems.
8. ____ In "An Introduction to Systems Design," it says "for further details see Freedom's Edge."
9. ____ In "An Introduction to Systems Design," it says "all references are to articles in Communications of the ACM".

6.6

You have been hired by a computer manufacturer to assess the security of an authentication scheme based on cryptographic synchronization. The scheme uses a hardware encryption/decryption (crypto) module at each end of the exposed communication line between a terminal and the computer. The encryption algorithm is certified to be (practically) unbreakable. The authentication scheme that the manufacturer proposes to use is as follows:

1. Bypassing the crypto module, user transmits personal identifier to computer.

2. User enables crypto module and inserts a personal key.

3. Computer enables crypto module and inserts key corresponding to user’s identifier received in step 1.

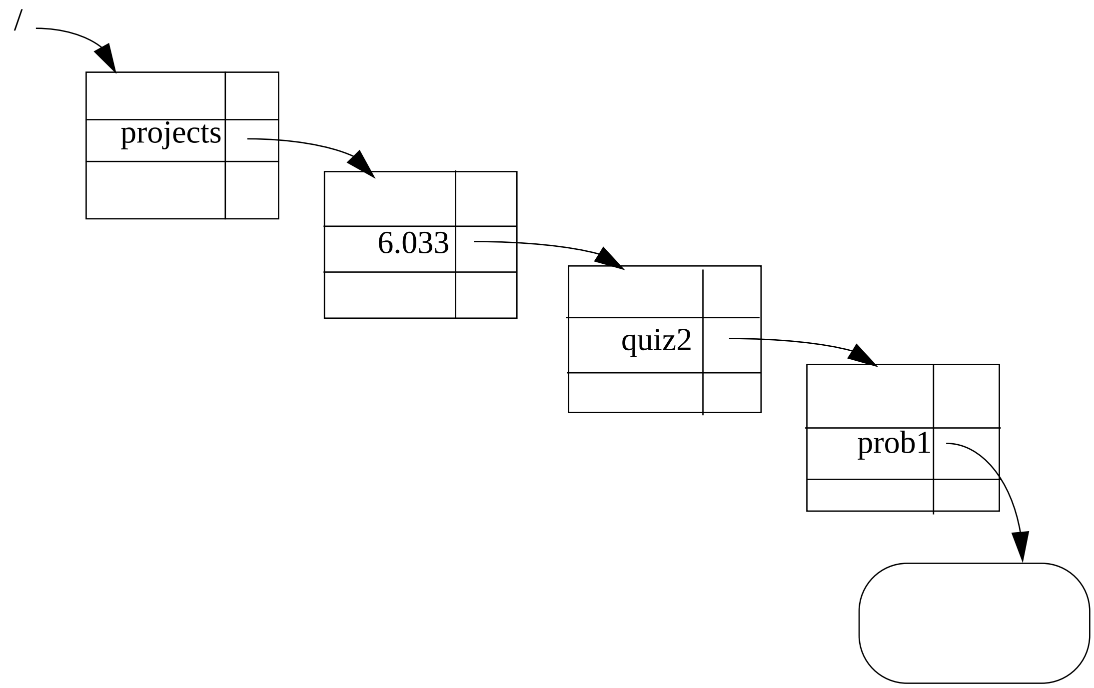
4. Using crypto module, computer transmits user’s identifier back to user. If this message decodes into the personal identifier, then user is sure of the identity of the computer.

5. Using the crypto module, the user transmits personal identifier back to computer. If this message decodes into the personal identifier transmitted in step 1, then computer is sure of user’s identity.

6. Communication between user and computer proceeds using crypto modules. Messages from user to computer contain consecutive sequence numbers (starting from 1 for each session). Messages from computer to user also contain consecutive sequence numbers (starting from 1 for each session).

What is your assessment of the security provided? Suggest methods for improving security.

1. *(10 points)* Consider the UNIX file system naming hierarchy illustrated below:



You have been handed the following path name:

/projects/6.033/quiz2/prob1

and you are about to resolve the third component of that path name, the name "quiz2".

1a. Circle the closure, and write the word "closure" next to the thing you have circled.

1b. Circle the context, and write the word "context" next to the thing you have circled.

2. *(25 points)* To obtain high throughput, communication applications pipeline messages: after sending the first packet of a message, they immediately send the next one without waiting for an acknowledgment of the first packet. A key question is how to establish how many packets to pipeline between a request and its acknowledgment (i.e., what is the window size).

2a. *(5 points)* Assume the client and the server are connected by an 800,000 byte/sec link. Also assume that the client and the server produce and consume packets at the same rate. Using the server's acknowledgments, the client measures the round-trip between itself and the server to be 10 milliseconds. If the client is sending 1000-byte packets, what is the smallest window size that allows the client to achieve 800,000 byte/sec throughput?

2b. *(5 points)* A popular scheme for establishing the window size in the Internet is *slow start*. In a simple version of slow start, a client starts with a small window size and increases the window size. Assume that the client starts with a window size of one packet. Also assume that for every packet, the server responds with an acknowledgment telling the client to double the window size. How long would it take for the client to know it has reached the maximum throughput?

2c. *(5 points)* Another scheme for establishing the window size is *fast start*. In fast start, a client starts by assuming a default large window size (say 8 packets) and sends the server a burst of that size. On the server's response, the window is adjusted to the size that is supplied by the server. If a client starts with a window size of 8, how long does it take for the client to know it has achieved the maximum throughput?

2d. *(10 points)* In the circumstances described above, fast start seems to be preferable. In what circumstances would it be preferable to use slow start over fast start? You may assume that one of the back-pressure techniques used in the Internet is dropping packets.

3. *(25 points)* Secure Inc. is developing an improved version of AFS, Secure AFS (SAFS), which automatically encrypts files to guarantee better privacy of information. When a request to store a file arrives, SAFS enciphers the file using the client's key. On arrival of a request to read a file, SAFS looks up the client key, deciphers the file, and sends the file back to the client. SAFS keeps for each client a separate key to encipher and decipher files.

3a. *(5 points)* The designers of Secure Inc. are wondering how long it would take to crack an enciphered file that is encrypted using RSA with 512-bit key, which is what is typically used today. To crack an RSA-enciphered file one has to factor the key. The designers know from the literature that factoring a 100 decimal digit number takes about 1 month using idle cycles from 300 3-MIPS SUN-3 workstations. It is estimated that factoring an additional 3 decimal digits roughly doubles the computation time needed. How many 3-MIPS computers are needed to factor a 155 decimal digit number (which corresponds to about 512 bits) in one month?

3b. *(5 points)* If processors are doubling computation performance per year, how many computers would it take to factor a 512-bit key in one month in the year 2000?

3c. *(5 points)* Let's assume that enciphering and deciphering can be done at 250 Kbyte/sec. How much would the throughput be reduced for reading files stored by SAFS, if the current maximum throughput without enciphering/deciphering is 800 Kbyte/sec? (You may assume that enciphering/deciphering cannot be pipelined with sending/receiving.)

3d. *(10 points)* Secure Inc. is also considering adding automatic compression of files to SAFS. Compression reduces redundancy of information in a file so that the file takes less disk space. Should they first compress files, then encipher them, or should they first encipher files and then compress them? Explain your answer briefly.

4. *(15 points)* Baybank is struggling to convince itself of the validity of a message it just received, and has asked your help in what to do next. So far, they know the following two facts to be true:

Louis says (Ben says (Transfer $1,000,000 to Alyssa))

Jim speaks for Ben

According to Ben's account representative, Ben's account has enough money for such a transaction, so if they can convince themselves that Ben really said that, they will do the transfer.

4a. *(5 points)* Which of the following things should they attempt to establish the truth of?

a. Louis speaks for Jim

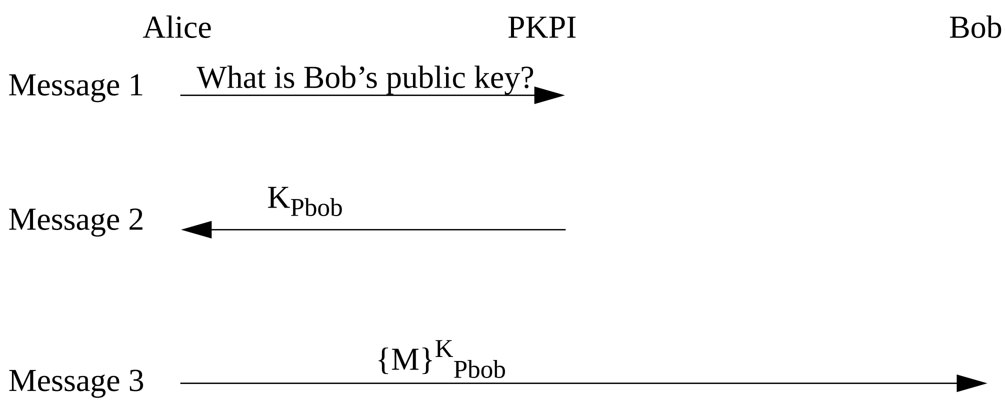
b. Ben speaks for Louis

c. Ben says (Jim speaks for Louis)

4b. *(10 points)* Why?

5. *(25 points)* Ben Bitdiddle and Louis Reasoner have founded a startup company, named Public Key Publication, Inc. (PKPI), whose business is distributing public keys. Their idea is that people who have a key-pair for use with a public-key system need a way of letting other people know the public key of their key-pair. Ben and Louis are not interested in creating keys, but just in acting as a public key distributor.

   Ben and Louis have designed the following protocol, in which Alice sends a private message to Bob. They need your help in debugging the protocol. K_{Pxyz} is the public key of principal xyz.



   Messages 1 and 2 constitute the PKPI protocol; message 3 is the beginning of Alice's protocol with Bob and is not under the control of PKPI; message 3 is shown here only to place the PKPI protocol in context.

5a. *(5 points)* Louis believes that Eve, the passive eavesdropper, will find that she cannot learn anything by overhearing the PKPI protocol in use. Give an argument that supports Louis' position, or an example demonstrating that Louis is mistaken.

5b. *(10 points)* Louis originally hoped that Lucifer, the active attacker, wouldn't be able to cause any problems, either, but since hearing the 6.033 lecture on the topic he is not sure. Give an example of an active attack that demonstrates that Louis needs to revise the PKPI protocol to protect against Lucifer.

5c. *(10 points)* Ben suggests that the protocol could be improved by changing Message 2. What should Message 2 contain, and how should it be enciphered, so that Alice can be confident that no one but Bob can decipher message 3?