CS 519
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Final Exam

January 13, 2003

Question 1. (*60 pts.*) Answer briefly each of the following questions:

a. What is the Kerckhoffs principle? Why is it significant?

b. What is the role of the so-called "compression function" in the general structure of a message digest (cryptographic hash) function?

c. What is the "guessable plaintext" problem in public key cryptography? How does the PKCS address it?

d. Consider the RSA algorithm where the modulus n is a large prime rather than a composite number. Would the encryption be secure? Why/why not?

e. Name one advantage and one disadvantage of using a challenge-response authentication protocol (with randomly generated keys) for user authentication instead of an ordinary password protocol.

f. Where a client and server share a password, it is always possible to use the password as the encryption key in a symmetric-key challenge-response protocol. What is the advantage of such an authentication protocol over ordinary password protocols? What is the advantage of EKE-type strong password protocols over this kind of challenge-response password protocols?

g. What are the three main classes of authentication protocols? (E.g., authentication by *what you know*, etc.) Name an advantage and a disadvantage of each.

h. Does Kerberos defend against off-line password guessing with eavesdropping? Why/why not?

i. Why, in your opinion, a separate SPI number is used for each direction of an IPsec-protected communication between two hosts?

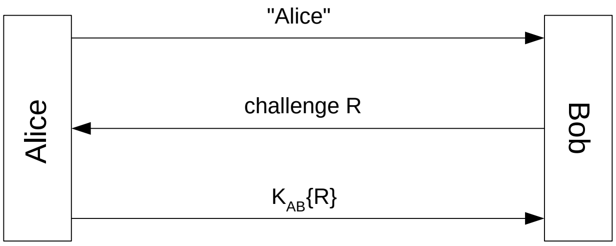
j. What is a virtual private network (VPN)? How can IPsec help creating a VPN? Which mode of IPsec operation would be used for this kind of application?

k. We know that the CBC-MAC is provably secure as a message authentication code—provided that the underlying block cipher is secure. Then, why does it fail in PEM?

l. What are the relative advantages and disadvantages of S/MIME and PGP? What are the environments that would favor each?

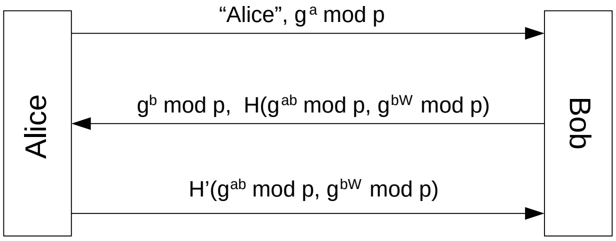
Turn the page

Question 2. (*15 pts.*) Consider the symmetric-key challenge-response protocol below where K_{AB} is the long term key Alice shares with Bob, and R is a random challenge.



If it is desired to establish a session key from this protocol, why would it be insecure to use $K_{AB}\{R+1\}$ as the session key? Describe an attack to demonstrate your point.

Question 3. (*25 pts.*) Consider the Augmented EKE type of protocol below where p and g are publicly known parameters, W is a weak secret derived from Alice's password, and the server Bob stores $g^W \bmod p$.


"Alice", g^a mod p
g^b mod p, H(g^ab mod p, g^bW mod p)
H'(g^ab mod p, g^bW mod p)
Alice
Bob

a. (*3 pts.*) Why is this protocol more secure than a similar protocol where Bob would store W rather than $g^W \bmod p$?

b. (*8 pts.*) Show the insecurity of this protocol with an attack where Trudy can do off-line guessing on Alice's password.

c. (*7 pts.*) This protocol can be made secure by making p a secret parameter known only to Alice and Bob.[1] Briefly argue why the attack in part (b) would not work against this modification. In such a protocol, why is it desirable to have p derived from the password rather than to have it as a separate, strong secret?

d. (*7 pts.*) Given that p is derived from the password, what safety check does Bob need to perform on Alice's initial message to preclude an impostor Trudy from doing an off-line guessing attack? (Hint: What if Trudy sends g for $g^a \bmod p$ in the first message?)

Good luck

[1] The generator g can be a public parameter, such as 2, that will work for all suitably generated p.