Name: ______________________________ UNI: _____________

COMS W4180: Network Security
March 2009

Rules

- Remember to write your name and UNI on the blue exam book.
- **Important: also write your name on this paper**
- You must turn in *both* the exam sheet and the blue book
- Books and notes are allowed during this examination; computers are not permitted.
- This is a time-limited test. All papers must be turned in 75 minutes after the beginning of the test.
- The points for each question are a rough guide to the effort I think is required. If you're spending more time or writing much more on a 10-point question than on a 20-point question, you may want to rethink your approach.
- The total points add up to 75 .
- Good luck, and may the Force be with you.

1		15
2		15
3		15
4		20
5		10
Total		75

Questions

1. (15 points) Alice wishes to have a secure conversation with Bob. She retrieves his certificate, and uses the public key to encrypt a session key. She then uses that session key (for a symmetric cipher) to talk with him. Some time *after* this conversation is over, the CA that issued Bob's certificate is compromised, and a fraudulent certificate for someone claiming to be Bob is issued. Are Alice's conversations with Bob at risk of being decrypted? Why or why not?

They are not at risk. You need Bob's real private key to decrypt the session key, and hence the communications; the CA would not have that. Future messages may be at risk, if Alice used the wrong certificate.

2. (15 points) Most IPsec ESP implementations use CBC mode. Someone has asserted that CBC mode isn't the only choice, and that CFB, OFB, and CTR modes are just as good. This is partially correct. In fact, OFB or CTR mode should not be used with static keys. That is, these modes are dangerous unless you use IKE or some other key management protocol. Why? (Note: assume that the ESP sequence number is used for the counter.)

If you use the same sequence number with the same key, the key stream will repeat, opening up an easy attack: XOR two ciphertexts together to cancel out the effect of the keystream, yielding the XOR of one plaintext with the other.

3. (15 points) Suppose I decide to administer the final as an online, take-home test. To prevent cheating, I insist that everyone get a certificate from the CA of their own choosing. Give two reasons why this won't achieve my goal.

(a) Do I trust those CAs that everyone choses? (b) The certificate is securing communications; it is not ensuring that there is no collaboration or other forms of cheating.

4. (20 points) You've just been appointed Chief Technology Officer for a major intelligence agency. Your spies in various countries want to email in their reports. The requirements are (a) that the reports be kept confidential, so that only the authorized recipient can read them; (b) that recipients be able to verify that the emails are from the right party; and (c) that the identity of the senders be hidden, to protect them from counterintelligence agents who may be eavesdropping. Explain what you would do in your design to achieve each of these three goals.

(a) Encrypt the messages using the recipient's public key to hide a session key. (b) Digitally sign the messages, using a per-spy secret key. (c) Sign first and encrypt the signed message, to hide the identity of the signer.

5. (10 points) You're a web security expert who has been building secure blogging sites; in particular, you've built mechanisms to restrict who can post comments. You've now been approached to design a bank's web site. Why is this a very different problem? (Note: remember that this is a 10-point question, and gauge your answer accordingly.)

(a) Much more is at risk; you need to take more precautions. (b) On blogs, anyone can comment; with a bank, you need to restrict user actions to their own accounts.