Questions from SampleFinal1 not covered in this term's exam: 3, 4, 9(b), 9(c)

C&O 487/687 Final Examination

April 21, 2015

Each problem is equally weighted. This exam has TWO pages. No calculators, aids, notes, or special materials permitted. Justify all answers and show all work.

If you need additional assumptions in order to complete a problem, state those assumptions clearly. Try to minimize the use of additional assumptions.

1. (a) Give 1-sentence informal definitions of the following fundamental goals of cryptography: confidentiality, data integrity, data origin authentication, non-repudiation.

   (b) Explain the difference between MAC algorithms and signature schemes.

2. Recall that RC4 is a stream cipher which, on input consisting of a secret key k, outputs a keystream RC4(k). The key stream is then used to encrypt a plaintext message by bitwise exclusive-or. What is the danger in using the same key k to encrypt two different plaintext messages?

3. (a) What type of interaction is required between the adversary and the legitimate user(s) in order to perform linear cryptanalysis? What goal can the adversary achieve under this interaction?

   (b) What type of interaction is required between the adversary and the legitimate user(s) in order to perform differential cryptanalysis? What goal can the adversary achieve under this interaction?

4. Recall the following notation, used in protocols such as DSA and Diffie-Hellman: p is an odd prime, q is a prime divisor of $p-1$, and $g \in \mathbb{Z}_p^*$ is an element of order q.

   Here is one method for generating g, given p and q:

   ```
   Repeat the following:
       Select $h \in \mathbb{Z}$ randomly from within the range $2 \leq h \leq p-1$,
       Compute $g = h^{(p-1)/q} \bmod p$.
   Until $g \neq 1$.
   Output($g$).
   ```

   Prove that this method works, i.e., prove that g has order q.

5. Why are RSA public and private keys so much longer than secret keys in a symmetric-key encryption scheme such as AES (for the same level of security)?

6. Recall the specification of (basic) hybrid encryption. We have a public-key cryptosystem $(\mathcal{G}, \mathcal{E}, \mathcal{D})$, and a symmetric-key cryptosystem (E, D) with key length ℓ. To send an encrypted message m, choose a random key $k \in \{0,1\}^\ell$, compute

   $$(c_1, c_2) = (\mathcal{E}(\text{pubkey}, k), E(k, m))$$

   and transmit this data to the recipient. To decrypt (c_1, c_2), compute

   $$m = D(\mathcal{D}(\text{privkey}, c_1), c_2).$$

   Throughout this problem, we will use the **one-time pad** as our symmetric-key cryptosystem.

   (a) Suppose that the public-key cryptosystem is insecure in such a way that an adversary intercepts a ciphertext and learns some partial (but not complete) information about k. What information can the adversary learn about m?

   (b) Suggest a practical modification of basic hybrid encryption which prevents the adversary from learning any information about m even if the public-key cryptosystem is compromised in the manner described in part (a).

7. What is *certificate revocation*? Why is it important to have certificate revocation in a public-key infrastructure (PKI)?

8. Discuss the security implications for Bitcoin if: (a) SHA-2 is broken, (b) ECDSA is broken.

9. In an implementation of RSA, we may choose to *blind* the ciphertext c as follows: after receiving the value of c, choose a random integer r, compute $c' = (c \cdot r^e) \bmod n$, and decrypt c' instead of c.

   (a) After decrypting c', how does the implementation recover the originally intended plaintext?

   (b) Does blinding protect against simple side-channel attacks, such as Simple Power Analysis (SPA)? Why or why not?

   (c) Does blinding protect against second-order side-channel attacks, such as Differential Power Analysis (DPA)? Why or why not?

10. Recall the specification of Full Domain Hash RSA (RSA-FDH):

    Key generation: Same as in basic RSA. Let ℓ denote the bitlength of n.

    Public parameters: A hash function $H\colon \{0,1\}^* \to \{0,1\}^\ell$.

    Signing: The message space is $\{0,1\}^*$. For any message $m \in \{0,1\}^*$, the signature of m is $s = H(m)^d \bmod n$.

    Verification: Given a signature s of a message m, compute $s^e \bmod n$ and check whether this value equals $H(m)$.

    (a) Describe how an adversary capable of mounting a known-message attack can forge Alice's signatures if H is not 2nd-preimage resistant.

    (b) Describe how an adversary capable of mounting a chosen-message attack can cheat if H is not collision resistant.

    (c) Describe how Alice can repudiate signatures if H is not collision resistant.