Family Name: . . . .

First Name: . . . .

Final Exam
Selected Topics on Security and Cryptography
July 2007

Warning:

- this exam consists of a survey and an exercise of same weight in the grade
- the survey consists of 3 series of 10 questions
- each series will be independently graded
- for each survey question there is one and only one correct answer
- any wrong answer may decrease the grade

1 Surveys

1.1 Communication Security

1. Bluetooth pairing is based on…
   □ bilinar mappings over elliptic curves.
   □ a short authenticated string.
   √ an ephemeral secret PIN code.
   □ an authenticated PIN code.

2. Tick the *false* assertion. Bluetooth…
   □ uses a stream cipher for encryption.
   √ has secure integrity protection for secure communication.
   □ has devices which use the same secret key with any other device.
   □ uses the SAFER+ block cipher in a one-way mode.

3. Bluetooth pairing…
   √ could be more secure if the link key was refreshed as often as possible.
   □ uses secure password-based authenticated key exchange.
   □ strongly protects anonymity in non-discoverable mode.
   □ uses sequence numbers in communication sessions.

4. Tick the *false* assertion. In connectable but non-discoverable mode, a device…
   √ only communicates using encryption.
   □ communicates over channels named from their Channel Access Code (CAC).
   □ can be addressed by using his Device Access Code (DAC).
   □ answers to queries by giving his identifier in clear.

5. Which of the followings is *not* an appropriate countermeasure?
   □ Put Bluetooth devices in a metalic bag.
   □ Use random 64-bit PINs.
   □ Use AES instead of E0.
   √ Hash the secret key before encryption.

6. Tick the *false* assertion: concerning the FMS attack…
   □ the secret key bytes $K[0], K[1], \ldots, K[p-1]$ must be known to recover $K[p]$, $p > 2$.
   □ to recover $K[3]$, the packet with an $IV = (3, 255, 17)$ is potentially useful.
   √ the first three bytes of the keystream must be known to recover $K[3]$.
   □ is not practical on SSL/TLS.

7. Which of the solutions below does *not* avoid FMS attack.
   □ Replace the first 16 bytes of the plaintext with random numbers.
   √ Add the SHA1 of the plaintext at the end of the packet before encrypting it.
   □ Filter IVs where the second byte is equal to 255.
   □ Replace the cipher RC4 with AES/CCM.

8. Tick the *false* assertion.
   - □ Two clients connected to the same wireless network, protected with WEP can use a different fixed secret key.
   - $\surd$ Because only a few bytes of the key change between two consecutive packets, the generated keystream is almost identical.
   - □ It is not recommended to use the authentication protocol defined in the WEP standard.
   - □ The integrity of the packet cannot be guaranteed by the CRC-32.

9. Tick the *true* assertion: The Klein attack…
   - □ uses the same weak *IV* class defined by the FMS attack.
   - □ is based on a weakness in the CRC-32.
   - $\surd$ need more known keystream bytes to recover the secret key.
   - □ uses only the *IV* to recover all the $K[p]$, $p > 3$.

10. Tick the *false* assertion: with WPA…
    - $\surd$ the replay attack is still possible.
    - □ the secret key used by RC4 is different for each packet.
    - □ the *IV* act as a counter.
    - □ the integrity, based on Michael is safer than CRC-32.

1.2 Provable Security and Hybrid Encryption

1. Which of the following security notions is the strongest one for a digital signature scheme?
   □ One-Wayness
   □ Semantic Security
   □ CCA-Security
   √ Existential Unforgeability

2. The ElGamal public-key cryptosystem is semantically secure under…
   □ the Computational Diffie-Hellman (CDH) problem.
   □ the discrete log (DL) problem.
   □ the assumption that factoring a large integer is hard.
   √ the Decisional Diffie-Hellman (DDH) problem.

3. Let A, B, and F be three events defined in some probability distribution and such that $A \wedge \overline{F} \Leftrightarrow B \wedge \overline{F}$. The *Difference Lemma* states that
   √ $|\Pr[A] - \Pr[B]| \leq \Pr[F]$
   □ $|\Pr[A] - \Pr[B]| \leq \Pr\left[\overline{F}\right]$
   □ $|\Pr[A] - \Pr[B]| \geq \Pr[F]$
   □ $|\Pr[A] - \Pr[B]| \geq \Pr\left[\overline{F}\right]$

4. Coron’s proof on the security of the Full Domain Hash (FDH) improves on that of Bellare and Rogaway by noting that it is better to include the challenge in the answer of *many* hash queries instead of just *one*. Tick the *false* assertion about this (brilliant) idea:
   √ It only applies to the FDH.
   □ It can also apply to the Rabin signature scheme.
   □ It can also apply to the Paillier signature scheme.
   □ It can also apply to the Gennaro-Halevi-Rabin signature scheme.

5. PSS stands for…
   √ probabilistic signature scheme.
   □ personal signature scheme.
   □ practical signature scheme.
   □ provably secure signature.

6. Tick the *false* assertion about PSS.
   □ PSS was introduced by Bellare and Rogaway.
   □ PSS has a tight security reduction.
   √ The security proof of PSS is due to Coron.
   □ PSS is different from the FDH.

7. Why does a weaker DEM suffice for IND-CCA TagKEM-DEM?
   √ TagKEM provides integrity to the tag
   □ KEM-DEM has too much redundancy
   □ TagKEM provides integrity to the encapsulated key
   □ DEM need no longer to generate a tag

8. What is the use of the tag input τ in TagKEM?
   □ to label the key encapsulation ψ so that integrity can be checked
   □ to provide integrity for the data encapsulation key dk
   ✓ to take the DEM calculation into account
   □ to provide privacy for the data encapsulation key dk

9. KDF stands for…
   ✓ Key Derivation Function.
   □ Key Data-File.
   □ Kentucky Chicken Fried.
   □ Krazy Cipher Feistel.

10. TCH stands for…
   □ Touring Club Hungary.
   □ Technologie-Centrum Hannover.
   ✓ Target Collision-Free.
   □ Tag Ciphertext Hash

1.3 Password-Based and Identity-Based Cryptography

1. Partition attacks…
   □ eliminate one password candidate per session.
   √ consist in decreasing the key space.
   □ are online active attacks.
   □ are played by musicians.

2. Which of the following cryptographic scheme was *not* proposed in an EKE variant in the original paper?
   □ RSA.
   □ Diffie-Hellman.
   □ ElGamal.
   √ Boneh-Franklin.

3. Which of the following must be prohibited?
   □ Use ephemeral Diffie-Hellman keys.
   □ Use ElGamal encryption.
   √ Send a public key in ASN.1 encrypted under the password.
   □ Use the same password twice.

4. Tick the *wrong* solution. Regarding online dictionary attacks against password-based authenticated key exchange protocols, we can…
   √ avoid it by encrypting the password.
   □ live with it.
   □ make sure that no better attack exists.
   □ audit logs to prevent them.

5. The EKE protocol was invented by…
   □ Boyko, MacKenzie, and Patel.
   √ Bellovin and Merritt.
   □ Bellare, Pointcheval, and Rogaway.
   □ Katz, Ostrovski, and Yung.

6. EKE stands for…
   □ Euskal Kultur Erakundeak.
   □ Exhaustive Key Enumeration.
   □ Extended Key Encryption.
   √ Encrypted Key Exchange.

7. Which of the following is *not* a password-based authenticated key exchange protocol.
   □ AMP.
   √ LLL.
   □ OKE.
   □ Jiang-Gong.

8. Certificateless Encryption uses…

   □ an email address to decrypt messages.

   √ two secret keys for decryption.

   □ a master key to encrypt data.

   □ a public-key infrastucture.

9. Fujisaki-Okamoto transforms…

   □ semantically secure encryption into an identity-based cryptosystem.

   □ public-key encryption into a digital signature scheme.

   □ identity-based encryption in the random oracle model into identity-based encryption in the standard model.

   √ one-way encryption into a cryptosystem which resists adaptive chosen ciphertext attacks.

10. Tick the *false* assertion about PSS. Pairings…

    √ are key agreements based on a secret PIN code which are used in identity-based encryption.

    □ are bilinear mappings.

    □ take two group elements as input and produce a third one as output.

    □ are the key ingredients that make identity-based encryption practical.

2 Exercise

EKE Issues

Passwords are strings w in a pretty small space $\mathcal{W}$. For any string $w \in \mathcal{W}$, we consider a permutation $\mathsf{SymEnc}_w : \{0,1\}^\ell \longrightarrow \{0,1\}^\ell$. We further assume a public-key cryptosystem $\mathsf{Gen}/\mathsf{Enc}/\mathsf{Dec}$ with a public key in $\{0,1\}^k$, a secret key in $\mathcal{K}$, plaintexts in $\{0,1\}^{\ell_p}$, and ciphertexts in $\{0,1\}^{\ell_c}$, where $\ell_p \leq \ell_c \leq \ell$ and $k \leq \ell$. Furthermore, bitstrings in $\{0,1\}^{\ell_c}$ and $\{0,1\}^k$ are implicitely considered as strings in $\{0,1\}^\ell$ by appending enough 0 bits.

We consider the following EKE protocol.

i. Alice first runs an algorithm Gen to generate a key pair $(K_p, K_s) \in \{0,1\}^k \times \mathcal{K}$, encrypts K_p with her password w by $a = \mathsf{SymEnc}_w(K_p)$, sends a to Bob;
ii. Bob receives a', applies $K'_p = \mathsf{SymEnc}_w^{-1}(a')$, picks a random $K' \in \{0,1\}^{\ell_p}$, encrypts K' by $b' = \mathsf{SymEnc}_w(\mathsf{Enc}_{K'_p}(K'))$, and returns b' to Alice;
iii. Alice receives b, decrypts by $K = \mathsf{Dec}_{K_s}(\mathsf{SymEnc}_w^{-1}(b))$.

To achieve explicit mutual authentication, the EKE protocol may continue with the following protocol.

iv. Alice picks a nonce N and sends $c = \mathsf{SymEnc}_K(N)$ to Bob.
v. Bob receives c', computes $N' = \mathsf{SymEnc}_{K'}^{-1}(c')$, and sends $d' = \mathsf{SymEnc}_{K'}(N'+1)$ to Alice.
vi. Alice receives d, checks $\mathsf{SymEnc}_K^{-1}(d) = N+1$, and sends $e = \mathsf{SymEnc}_K(N+2)$ to Bob.
vii. Bob receives e' and checks $\mathsf{SymEnc}_{K'}^{-1}(e') = N'+2$.

$$\begin{array}{rcl}
\textbf{Alice} & & \textbf{Bob} \\
\textbf{password}: w & & \textbf{password}: w \\
\hline
(K_p, K_s) \leftarrow \mathsf{Gen} & & \\
a = \mathsf{SymEnc}_w(K_p) & \xrightarrow{\quad a \quad} & K'_p = \mathsf{SymEnc}_w^{-1}(a') \\
 & & \text{pick } K' \\
K = \mathsf{Dec}_{K_s}(\mathsf{SymEnc}_w^{-1}(b)) & \xleftarrow{\quad b \quad} & b' = \mathsf{SymEnc}_w(\mathsf{Enc}_{K'_p}(K')) \\
\hline
\text{pick } N & & \\
c = \mathsf{SymEnc}_K(N) & \xrightarrow{\quad c \quad} & N' = \mathsf{SymEnc}_{K'}^{-1}(c') \\
N+1 \overset{?}{=} \mathsf{SymEnc}_K^{-1}(d) & \xleftarrow{\quad d \quad} & d' = \mathsf{SymEnc}_{K'}(N'+1) \\
e = \mathsf{SymEnc}_K(N+2) & \xrightarrow{\quad e \quad} & N'+2 \overset{?}{=} \mathsf{SymEnc}_{K'}^{-1}(c') \\
\hline
\textbf{output}: K & & \textbf{output}: K'
\end{array}$$

1. If $\ell_c < \ell$, show that an adversary observing a protocol session can eliminate at least half of all possible guesses for w. Deduce an offline exhaustive search.

In what follows we will assume $\ell_c = \ell$ to avoid this attack.

2. If $k < \ell$, show that an adversary observing a protocol session can eliminate at least half of all possible guesses for w. Deduce an offline exhaustive search.
   In what follows we will assume $k = \ell$ to avoid this attack.

3. More generally, we assume there is an algorithm $L : \{0,1\}^k \longrightarrow \{0,1\}$ such that

$$\Pr[L(K_p) = 1 | (K_p, K_s) \leftarrow \mathsf{Gen}] = 1$$
$$\Pr[L(K_p) = 1 | K_p \overset{\mathsf{uniform}}{\leftarrow} \{0,1\}^k] < \tfrac{1}{2}.$$

Propose another attack.

4. Instead of the proposed protocol, Alice prefers to send K_p in clear. By impersonating Alice (i.e. by running an active attack), show that we can get information to run an offline exhaustive search.

5. Alice has an account on two servers $\mathcal{B}_1$ and $\mathcal{B}_1$ on which she uses passwords w_1 and w_2 respectively. She lazily implements EKE in such a way that she does not generate an ephemeral (K_p, K_s) pair for every session but rather uses a static one. Show how to run an offline exhaustive search on w_1 and w_2 after observing two protocol sessions.
(Hint: remember meet-in-the-middle attacks.)