Applied Cryptography Final Examination

Spring Semester 2022

(263-4660-00L)

K.G. Paterson

Student name: _____

Legi number: _____

Examination Rules:

(a) **DO NOT TURN OVER THIS PAGE UNTIL INSTRUCTED TO DO SO BY AN EXAMINER.**

(b) Closed-book, written exam, 120 minutes total.

(c) If you feel disturbed or have questions about the exam, raise your hand to call an assistant.

(d) You are permitted to leave the exam early, but not within the last 10 minutes of the exam. If you wish to leave, please raise your hand and wait for an assistant.

(e) There are three problems in the exam, worth 25 marks each. You should attempt as many parts as you can, but you do not need to complete every part of every problem to obtain the best possible grade.

(f) Read all the problems before beginning.

(g) Write your name and legi number at the top of this title page and each sheet of paper that you use.

(h) Start each problem on a new sheet of paper.

(i) Write as clearly as you can and show all your work. For some questions, you may get partial credit even if the end result is wrong due to a calculation error.

(j) Write with a black or blue pen (no pencil, no green or red ink).

(k) Turn off your mobile phone. No electronic devices are allowed on desks, except for watches. Smartwatches are not permitted.

Problem	1	2	3	$\sum$
Max. Points	25	25	25	75
Points				
Signature				

Problem 1 (Authenticated Encryption). Recall that an Authenticated Encryption (AE) scheme consists of a triple of algorithms (`KGen`, `Enc`, `Dec`).

(a) Security for AE schemes is defined in terms of the combination of two security notions: indistinguishability under chosen plaintext attacks (IND-CPA security), and integrity of ciphertexts (INT-CTXT security). Give definitions of these two security notions, using diagrams or pseudo-code to illustrate your answer, as you prefer. In each case, define the adversary's advantage, and state what it means for an AE scheme to be secure in terms of the resources consumed by the adversary. [6 marks]

(b) One approach to building AE schemes is to compose a symmetric encryption scheme and a MAC scheme. There are three options for performing this generic composition: EtM, MtE and E&M. Given a symmetric encryption scheme `SE` with algorithms (`SE.KGen`, `SE.Enc`, `SE.Dec`) and a MAC scheme `MAC` with algorithms (`MAC.KGen`, `MAC.Tag`, `MAC.Vfy`), write pseudo-code describing the encryption and decryption algorithms for the EtM and E&M options (so 4 algorithms in total). [4 marks]

(c) Give a proof showing that if an IND-CPA-secure symmetric encryption scheme `SE` and a SUF-CMA-secure MAC scheme `MAC` are used, then the EtM construction does achieve AE security. [8 marks]

(d) OpenSSH supports the generic EtM construction, allowing several different options for the symmetric encryption and MAC components. In OpenSSH versions 5.2 to 7.2, the decryption algorithm for EtM proceeded as follows:

```
def Dec(ciphertext):
    C = ciphertext[:-MAC.tag_length]
    t = ciphertext[-MAC.tag_length:]

    t_p = MAC.Tag(MAC.K, C)

    M = SE.Dec(SE.K, C)

    if t == t_p:
        return M
    else
        raise MACError
```

i) Describe how this approach to decryption differs from how you defined decryption for EtM in part b) above. [1 mark]

ii) Suppose `SE` is instantiated using CBC mode of a PRP-secure block cipher in combination with the simplified TLS padding scheme (in which data is byte-aligned and the possible padding patterns are `0x00`, `0x01`||`0x01`, ...). Provide

an evaluation of the security of the OpenSSH EtM construction in this case. (Hint: consider what may happen in the event of an error arising during CBC mode decryption.) [4 marks]

iii) Suppose `SE` is instantiated using CTR mode of a PRP-secure block cipher, in such a way that counters are never reused. Provide a brief evaluation of the security of the OpenSSH EtM construction in this case. [2 marks]

Problem 2 (Public Key Encryption). Recall that a PKE scheme consists of a triple of algorithms $(\texttt{KGen}, \texttt{Enc}, \texttt{Dec})$, while a Key Encapsulation Mechanism (KEM) consists of a triple of algorithms $(\texttt{KGen}, \texttt{Encap}, \texttt{Decap})$.

(a) The standard notion of security for a PKE scheme is indistinguishability under chosen ciphertext attack, or IND-CCA for short. Define this security notion in terms of a security game played between a challenger and an adversary. As part of your answer, define what it means for a PKE scheme to be (q_d, t, ϵ)-IND-CCA secure. [4 marks]

(b) Briefly explain how the IND-CCA security notion for a KEM differs from that for a PKE scheme. [2 marks]

(c) Explain why the weaker IND-CPA security notions are insufficient for PKE schemes and KEMs in practice. [2 marks]

(d) A PKE scheme can be generically constructed from a KEM and an AE scheme with algorithms $(\texttt{KGen}_{\text{AE}}, \texttt{Enc}_{\text{AE}}, \texttt{Dec}_{\text{AE}})$. Describe the construction, showing how each algorithm of the PKE scheme is obtained by using algorithms from the KEM and the AE scheme. [3 marks]

(e) Consider the following RSA-based KEM:

$\texttt{KGen}$: perform textbook RSA key generation to produce a public key $pk = (e, N)$ and a private key $sk = (d, N)$. Here $N = pq$ where p and q are primes of a suitable size and (d, e) are such that $de = 1 \bmod (p-1)(q-1)$. We suppose N has n bits where n is a multiple of 8 and $n \geq 2048$.

$\texttt{Encap}((e, N))$: on input public key (e, N):

1. set $K \leftarrow_{\$} \{0,1\}^{256}$, $R \leftarrow_{\$} \{0,1\}^{(n-8)-256}$, $M = \texttt{0x00}||R||K$;
2. interpret M as a big-endian (that is, with most significant bits on the left) integer mod N;
3. compute $C = M^e \bmod N$; output (C, K).

$\texttt{Decap}(C, (d, N))$: on input encapsulation C and private key (d, N):

1. compute $M = C^d \bmod N$;
2. interpret M as a big-endian n-bit array, and write $B||R||K = M$ where B has 8 bits and K has 256 bits;
3. if $B = \texttt{0x00}$ then return K, else return an error indicating decapsulation failure.

i) Show that this KEM is not IND-CCA secure by exhibiting an attack against it in the IND-CCA security model; as part of your answer state and justify the advantage and query complexity of your attack. Full credit will be given for an attack that makes just one query to the decapsulation oracle. [6 marks]

ii) Briefly explain how you would construct an IND-CCA secure KEM in the RSA setting. [2 marks]

(f) Describe the main advantage of Elliptic Curve Cryptography (ECC) in comparison to RSA-based cryptography. [2 marks]

(g) ECC was invented in the mid-1980s but took until the mid-2010s to become widely deployed. Discuss the reasons for this 30-year delay in the take-up of ECC. [4 marks]

Problem 3 (Key Exchange).

(a) What security properties does an authenticated key exchange protocol require from its underlying communication network to securely operate? How are these assumptions captured by security models for key exchange? [2 marks]

(b) Describe the unauthenticated Diffie–Hellman two-party key exchange protocol based on a cyclic group $\mathbb{G} = \langle g \rangle$ of order q and a key derivation function KDF. Write down the operations performed by each party in order to agree on a shared, uniform session key K. You may use a diagram to describe the protocol. [3 marks]

(c) Explain why the unauthenticated Diffie–Hellman key exchange protocol does not provide security against an *active* adversary by briefly describing an attack on the protocol. [2 marks]

(d) Security against active adversaries can be achieved using entity authentication. Briefly describe one method to add entity authentication to an unauthenticated key exchange protocol. State the cryptographic primitives involved and potential knowledge of keys assumed. You only need to describe one direction, for example, how to unilaterally authenticate the responder to the initiator. [3 marks]

(e) The unauthenticated Diffie–Hellman key exchange protocol based on a cyclic group $\mathbb{G} = \langle g \rangle$ of order q and a key derivation function KDF from (b) achieves key secrecy against passive adversaries ("passive key secrecy") under appropriate assumptions on $\mathbb{G}$ and KDF.

Informally, passive key secrecy is defined as:

> "Given the transcript of a single execution of the key exchange protocol, an adversary cannot distinguish the session key established in that execution from a key sampled uniformly at random from the session key space $\mathcal{K}$."

1) Complete the following security game KS by filling in the gaps to formalize passive key secrecy for unauthenticated Diffie–Hellman key exchange. [4 marks]

Game $\mathsf{KS}(\mathcal{A}, \mathbb{G}, \mathsf{KDF})$:

1 $b \leftarrow\!\!\$\ \{0,1\}$

2 _____ // Party A's local computation.

3 $\mathsf{trans}_A \leftarrow$ _____ // Party A's share of the communication transcript ("What A sends").

4 _____ // Party B's local computation.

5 $\mathsf{trans}_B \leftarrow$ _____ // Party B's share of the communication transcript ("What B sends").

6 $K_0 \leftarrow \mathsf{KDF}($_____$)$ // Computation of the "real" session key.

7 _____ // Computation of the "random" key.

8 $b' \leftarrow\!\!\$\ \mathcal{A}(\mathsf{trans}_A, \mathsf{trans}_B,$ _____$)$ // Challenge for the adversary.

9 Return $(b' = b)$

Complete the definition: The advantage of $\mathcal{A}$ in breaking passive key secrecy in KS is defined as

$$\mathbf{Adv}^{\mathsf{KS}}_{\mathbb{G},\mathsf{KDF}}(\mathcal{A}) = \_\_\_\_\_$$

2) Sketch a security proof for the passive key secrecy of the unauthenticated Diffie–Hellman key exchange protocol from (b).
Clearly state the security assumptions you make. [6 marks]

(f) One place where key exchange is used in practice is in the "ratcheting" mechanisms of the Signal messaging protocol. Signal uses two distinct ratcheting mechanisms.

1) Name them and briefly describe their respective core idea. [3 marks]

2) Briefly state the main difference in terms of security they provide. [2 marks]