Applied Cryptography SS2020 – Exam

(263-4660-00L)

K.G. Paterson

Examination Rules:

1. Written exam, 120 minutes total.
2. This document contains 4 pages in addition to this cover page.
3. There are 4 questions. Each question begins on a new page. Attempt them all.
4. Write all your answers on A4 sheets of paper. Put your name and student number at the top of each sheet. Number the sheets. Start your answer to each question on a new sheet. Put your declaration of originality on its own on the final sheet.
5. Books, calculators, computers and communication devices are not permitted.
6. In the event of any problems, immediately attract the attention of an assistant by using the "raise hand" feature in Zoom.
7. Answers will only be evaluated if they are readable.
8. Write with a black or blue pen (no pencil, no green or red colour).
9. Show all your work. For some questions, you may get partial credit even if the end result is wrong due to a calculation mistake.

1. $\boxed{\text{25 points}}$ This question is about PRFs and nonce-based MAC algorithms.

   (a) $\boxed{\text{6 points}}$ One can construct a MAC scheme from a PRF $F : \{0,1\}^k \times \mathcal{X} \to \mathcal{T}$ by defining the Tag algorithm as follows: for $K \in \{0,1\}^k$ and $M \in \mathcal{X}$, define $\mathrm{Tag}(K, M) = F(K, M)$. Give a sketch proof that the resulting scheme is strongly unforgeable, stating a concrete security bound on the advantage of a MAC adversary A in terms of the PRF advantage of a related adversary B. (You may use a security model in which the MAC adversary does not have access to a verification oracle.)

   (b) $\boxed{\text{2 points}}$ Suppose H is a hash function from a set $\mathcal{X}'$ to the set $\mathcal{X}$. Show how to combine H and F (as in part a) above) to build a MAC scheme for messages in $\mathcal{X}'$. State what property you require of H for the resulting MAC scheme to be strongly unforgeable. (No proof is required.)

   (c) $\boxed{\text{2 points}}$ Explain, in the context of cryptography, what a nonce is and why it can be attractive to developers to use nonce-based schemes.

   (d) $\boxed{\text{4 points}}$ Define the syntax and correctness of a nonce-based MAC scheme in terms of its constituent algorithms $(\mathrm{KGen}, \mathrm{Tag}, \mathrm{Vfy})$.

   (e) $\boxed{\text{3 points}}$ Briefly define a suitable security notion for nonce-based MAC schemes.

   (f) $\boxed{\text{4 points}}$ Recall that an ϵ-Difference Unpredictable Hash Function (ϵ-DUHF) is a keyed hash function $H : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ such that, for all $\delta \in \mathcal{T}$, and all $m_1, m_2 \in \mathcal{M}$:

   $$\Pr_K[H(K, m_1) - H(K, m_2) = \delta] \leq \epsilon.$$

   Here "$-$" denotes the inverse of some group operation "$+$" on the set $\mathcal{T}$ and the probability is taken over a uniform distribution on $K \in \mathcal{K}$.

   The Carter-Wegman construction builds a nonce-based MAC scheme by combining a PRF F with outputs in $\mathcal{T}$ and an ϵ-DUHF H. The MAC tags are of the form $F(K_1, N) + H(K_2, M)$, where N is the nonce, M is the message and K_1, K_2 are keys.

   Explain at a high-level why this MAC is secure, by considering the two cases where i) the adversary outputs a forgery for a nonce not used in any of its tag oracle queries, and ii) the adversary outputs a forgery for a nonce that was previously used in one of its tag oracle queries.

   (g) $\boxed{\text{4 points}}$ Recall that $\mathrm{H_{xpoly}}$ is the DUHF in which keys K are elements from some field $\mathbb{F}$, messages are vectors $(a_1, \ldots, a_v)$ over the same field, and:

   $$\mathrm{H_{xpoly}}(K, (a_1, \ldots, a_v)) = K^{v+1} + a_1 K^v + \cdots + a_v K.$$

   A developer mis-reads the Carter-Wegman specification and instead implements the tag algorithm by concatenating the PRF and $\mathrm{H_{xpoly}}$ outputs, adjusting the verification algorithm to match. Show that an adversary, given access to the tag oracle for just two chosen nonce and message pairs, can then easily forge valid MAC tags for *any* message in this scheme.

2. $\boxed{\text{25 points}}$ This question concerns Authenticated Encryption (AE) and the use of generic composition to achieve it.

   (a) $\boxed{\text{4 points}}$ 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 to illustrate your answer if you wish. 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.

   (b) $\boxed{\text{6 points}}$ One way to build an AE scheme is to compose a symmetric encryption scheme and a MAC scheme. There are three options for doing so: EtM, MtE and E&M. Given a symmetric encryption scheme with algorithms $(\mathrm{KGen}_\mathrm{E}, \mathrm{Enc}, \mathrm{Dec})$ and a MAC scheme with algorithms $(\mathrm{KGen}_\mathrm{M}, \mathrm{Tag}, \mathrm{Vfy})$, describe each of these options.

   (c) $\boxed{\text{2 points}}$ The E&M option is not *generically secure*. Explain what is meant by *generic security* in this context, and demonstrate that E&M does not achieve it.

   (d) $\boxed{\text{6 points}}$ Give a sketch proof that the EtM construction is generically secure as an AE scheme. State carefully any security assumptions that you make about the component schemes.

   (e) $\boxed{\text{5 points}}$ Show by means of an example involving CBC-mode encryption and CBC-MAC that the EtM construction can fail to provide AE security if the same key is used in both the symmetric encryption and MAC scheme components. You may consider a restricted message space in your scheme, but you must state clearly what message space your EtM example supports. You should show that your EtM example fails to achieve both confidentiality and integrity, giving details of attacks and adversarial advantages against both notions for your specific EtM example. You do *not* need to establish the security of the symmetric encryption and MAC scheme components, but they should meet appropriate security notions.

   (f) $\boxed{\text{2 points}}$ Explain how a Key Derivation Function could be used to address the issues arising in your EtM example.

3. $\boxed{\text{25 points}}$ This question is about RSA encryption.

   (a) $\boxed{\text{4 points}}$ A *public key encryption (PKE) scheme* consists of a triple of algorithms $(\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$. Describe the function of each of these algorithms and explain what is meant by the *correctness* of a PKE scheme.

   (b) $\boxed{\text{4 points}}$ 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, taking care to define what it means for a scheme to be (q_d, t, ϵ)-secure according to this notion. Explain why it is important in practice that a PKE scheme should satisfy the notion.

   (c) $\boxed{\text{2 points}}$ Explain why a PKE scheme in which Enc is deterministic cannot be IND-CCA secure.

   (d) $\boxed{\text{3 points}}$ The textbook RSA encryption scheme has ciphertexts C in which $C = M^e \bmod N$. Here M is a message interpreted as a number between 0 and $N-1$, (N, e) is the public encryption key, d is the private decryption key, and $N = pq$ is a product of two primes p and q.

      i) Describe the algorithm Dec for this scheme.

      ii) Explain the relationship between the security of this scheme and the integer factorisation problem.

   (e) $\boxed{\text{10 points}}$ A developer proposes to use the textbook RSA-based encryption scheme in a protocol to transport a 256-bit session key K from a client to a remote server over a network. The developer knows he should avoid small e and also use a hash function to break up algebraic relationships. So he proceeds as follows. The client selects R uniformly at random from $\{0,1\}^{1024}$, interprets R as a 1024-bit integer, and then computes an RSA ciphertext C via $C = R^e \bmod N$. Here N is a 3072-bit RSA modulus and $e = 2^{16} + 1$. Ciphertext C is then sent to the server over the network. The server uses textbook RSA decryption on C to recover an integer R', truncates R' to its least significant 1024 bits, and sets the key K to the 256-bit value SHA-256(R'). The server then uses K in an Authenticated Encryption (AE) scheme to encrypt a fixed message that is sent back to the client; this message is intended to confirm that the server has successfully obtained the session key. The key K is also used to protect subsequent exchanges of data between the client and server.

      The developer claims that his scheme is secure because it encrypts random values, hashes them to make the session keys using a collision-resistant hash function, avoids small e, and uses a large modulus.

      Disprove this claim by describing a practical attack that recovers K for any session. Your answer should include a discussion of the practicality and an analysis of the efficiency of your attack. (Hint: let C^* denote the RSA ciphertext in a target session and consider the server's behaviour when receiving ciphertexts of the form $2^{et}C^* \bmod N$ for suitable values of t.)

   (f) $\boxed{\text{2 points}}$ The developer asks for your help to modify his protocol to make it secure. Explain how to do this in a minimally invasive way.

4. 25 points This question concerns the TLS protocol.

   (a) 4 points What are the main security goals of the TLS Protocol?

   (b) 4 points Describe at a high level the operations of the TLS Handshake and TLS Record Protocols, and explain how they relate to one another.

   (c) 4 points The TLS Handshake Protocol has cipher suite negotiation as a feature. Explain what this feature accomplishes, why it is important, and the mechanism by which it is performed in TLS.

   (d) 4 points TLS in versions prior to TLS 1.3 supports EXPORT cipher suites, for example TLS_RSA_EXPORT_WITH_RC4_40_MD5. What dangers do such cipher suites entail?

   (e) 4 points TLS 1.3 represents a major overhaul of the TLS protocol. Explain why this overhaul was needed and describe the main enhancements of TLS 1.3 as compared to earlier versions of the protocol.

   (f) 5 points Describe the 0-RTT feature of TLS 1.3. Your answer should describe its benefits, its operation, and its security weaknesses.

End of Exam Paper