COMP547A Homework set #4

Due Thursday December 1st, 2022, 23:59

Exercises (from Katz and Lindell's book)

[5%]

4.7 Let F be a pseudorandom function. Show that the following MAC for messages of length $2n$ is insecure: Gen outputs a uniform $k \in \{0,1\}^n$. To authenticate a message $m_1 \| m_2$ with $|m_1| = |m_2| = n$, compute the tag $F_k(m_1) \| F_k(F_k(m_2))$.

[5%]

[5%]

[5%]

[5%]

4.27 Define an appropriate notion of a ε-secure *two-time* MAC, and give a construction that meets your definition.

HOMEMADE Question: Achieving Rivest's private-key encryption from a Mac

[5%]

Provide a security definition of a **Mac** that makes the (bit-by-bit) private-key encryption scheme that Rivest described secure in the sense of indistinguishability in the presence of an eavesdropper.

More on back…

12.

[1%]

[4%]

Hint: Prove that if "not CPA-secure" then "DDH problem is efficiently solved".

[5%]

[5%]

[5%]

[5%]

More on back…

[5%] 13.1 Show that Construction 4.7 for constructing a variable-length MAC from any fixed-length MAC can also be used (with appropriate modifications) to construct a signature scheme for arbitrary-length messages from any signature scheme for messages of fixed length $\ell(n) \geq n$.

[5%]

[5%]

[5%]

[5%]

[5%]

HOMEMADE

Alice and Bob are a bit confused. They are ignature scheme as a **Mac**. Let $\Pi = (\mathrm{Gen}, \mathrm{Sig}$ terministic digital signature scheme (such as hashed RSA f $\mathrm{Gen}(1^n)$ to obtain (p_k, s_k) but only share and use s_k as the private-key of a **Mac**.

[5%] (A) Let $\Pi' = (\mathrm{Gen}', \mathrm{Mac}', \mathrm{Vrfy}')$ be the **Mac** resulting from this idea. Used as a **Mac** they simply set $t := \mathrm{Mac}'_{sk}(m) := \mathrm{Sign}_{sk}(m)$. However, since they only use s_k, how will the receiver verify the message-tag pair (m, t) ? In other words, what is $\mathrm{Vrfy}'_{sk}(m, t)$? Why did I underlined the word "*deterministic*" above ?

[5%] (B) Show that if Π is a digital signature scheme existentially unforgeable under an adaptive chosen-message attack then Π' is a Mac existentially unforgeable under an adaptive chosen-message attack (whether p_k is made public or not).

[5%] (C) Image that Alice and Bob use Π' as above, and that p_k is disclosed publicly. Explain how this defeats Rivest's argument seen in class that private-key authentication implies private-key encryption.

More on back…