به نام آن که هیچ رمزی برایش پوشیده نیست

تمرین سری ۵ رمزنگاری

دانشکده ریاضی، آمار و علوم کامپیوتر

رمزنگاری-ترم اول سال تحصیلی ۹۵-۹۴

تاریخ تحویل: یکشنبه ۹۴/۱۰/۲۰

سؤال ۱

فرض کنید خانواده $F = \{F_k : k \leftarrow \{0,1\}^n\}$ شبه تصادفی باشد. MAC زیر را که فقط برای پیام‌هایی با طول $2n$ مورد استفاده قرار می‌گیرد، در نظر بگیرید.

$$k \in \{0,1\}^n, \quad M = m_1||m_2 \in \{0,1\}^{2n}; \quad t = Mac_k(M) = (F_k(m_1), F_k(F_k(m_2))$$

۱. الگوریتم $\text{Vrfy}_k(M,t)$ چگونه کار می‌کند؟

۲. آیا این سامانه MAC امن است؟

سؤال ۲

فرض کنید $f_k : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ خانواده‌ای (از توابع) شبه تصادفی باشد، MAC زیر را که برای پیام‌هایی با طول دلخواه استفاده می‌شود در نظر بگیرید: در الگوریتم مورد نظر $[i]_{\frac{n}{2}}$ نمایش باینری

$$\text{pad}(M) = M||10\cdots0 = m_1 m_2 \cdots m_d, |m_i| = \frac{n}{2}$$

$$t_i = f_k([i]_{\frac{n}{2}}||m_i)$$

$$\langle t_1, \cdots, t_d \rangle \leftarrow \text{Mac}_k(M)$$

عدد i توسط یک رشته‌ی $\frac{n}{2}$ بیتی است.
آیا این سامنه امن است؟

سؤال ۳

اگر در الگوریتم سؤال ۲ خروجی MAC_k را برابر با $t_1 \oplus t_2 \oplus \ldots \oplus t_d$ در نظر بگیریم آیا سامانه MAC جدید امن خواهد بود؟

سؤال ۴

فرض کنید $f_k : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ خانواده‌ای (از توابع) شبه تصادفی باشد، امنیت MAC زیر را مورد بررسی قرار دهید. در این الگوریتم $[i]_{\frac{n}{3}}$ نمایش باینری عدد i توسط یک رشته‌ی $\frac{n}{3}$ بیتی است.

$$|m| = \ell$$

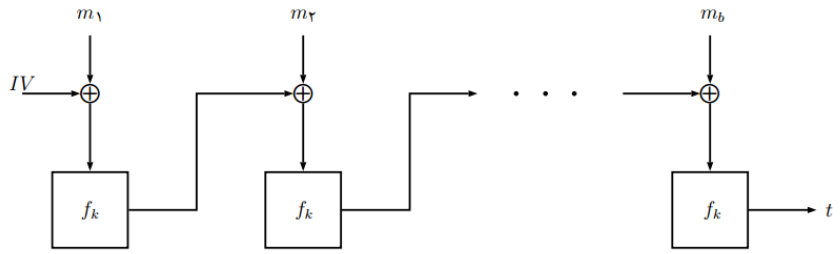
$$\text{pad}(M) = M||10\cdots0 = m_1 m_2 \cdots m_d, |m_i| = \frac{n}{3}$$

$$t_i = f_k([i]_{\frac{n}{3}}||m_i||[\ell]_{\frac{n}{3}})$$

$$\langle t_1, \cdots, t_d \rangle \leftarrow \mathsf{Mac}_k(M)$$

سؤال ۵

$CBC-MAC$ زیر را برای برچسب‌گذاری پیام‌های با طول دلخواه را در نظر بگیرید: در این الگوریتم IV



یک مقدار تصادفی است و عمل پدینگ با قرار دادن بیت ۱ و سپس به اندازه کافی بیت صفر تا رسیدن طول پیام حاصله به مضربی از طول قالب (n) انجام می‌شود. خروجی الگوریتم فوق (برچسب) [1] عبارت است از $Mac_k(m) =< IV, t >$. آیا ساختار فوق می‌تواند یک MAC امن باشد؟

سؤال ۶

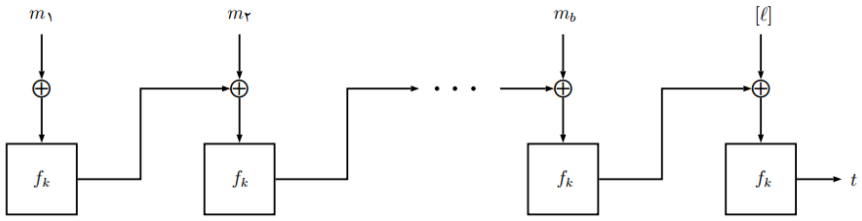
MAC زیر را در نظر بگیرید: در الگوریتم مذکور $< l >$ نمایش باینری n بیتی عدد l به عنوان طول پیام قبل از پدینگ است.

(عمل پدینگ پیام مثل سؤال ۵ انجام می‌شود و طول پیام ورودی دلخواه است)

۱. الگوریتم $\text{Vrfy}(M,t)$ چگونه کار می‌کند؟

۲. نشان دهید MAC معرفی شده ناامن است.

[1] Tag



سؤال ۸

فرض کنید $F_k(m)$ یک MAC امن برای پیام‌های با طول n باشد. (اصلا لزومی ندارد $F_k(.)$ جایگشت شبه تصادفی باشد). در این صورت آیا آلگوریتم CBC-MAC زیر برای حالتی که طول پیام‌های ورودی ثابت (برای مثال طولی برابر با $l = l(n)$) باشد، امن است؟

Mac: on input a key $k \in \{0,1\}^n$ and a message m of length $\ell(n) \cdot n$, do the following (we set $\ell = \ell(n)$ in what follows):

1. Parse m as $m = m_1, \ldots, m_\ell$ where each m_i is of length n.
2. Set $t_0 := 0^n$. Then, for $i = 1$ to ℓ:
   Set $t_i := F_k(t_{i-1} \oplus m_i)$.

Output t_ℓ as the tag.

Vrfy: on input a key $k \in \{0,1\}^n$, a message m, and a tag t, do: If m is not of length $\ell(n) \cdot n$ then output 0. Otherwise, output 1 if and only if $t \stackrel{?}{=} \mathsf{Mac}_k(m)$.

سؤال ۹

الگوریتم CBC-MAC در سؤال ۸ را در نظر بگیرید، تغییرات زیر را بر این الگوریتم اعمال می‌کنیم:

۱. فرض می‌کنیم $F_k(.)$ تابع شبه تصادفی باشد.

۲. طول پیام وردی متغیّر ولی حتما مضربی از طول قالب است. (در سؤال قبل l ثابت بود ولی در این سؤال متغیّر و مضربی از n (طول قالب) است.)

۳. برای محاسبه $\mathrm{MAC}_k(M)$ در ابتدا مقدار $k^* = F_k(l)$ ($l = |M|$) محاسبه شده سپس برای تولید برچسب t از همان الگوریتم سؤال ۸ تحت کلید k^* استفاده می‌کنیم.

نشان دهید الگوریتم جدید امن است.