دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

عنوان: تکلیف اول درس مهندسی فناوری اطلاعات

نام و نام خانوادگی: علیرضا ابره فروش

شماره دانشجویی: ۹۸۱۶۶۰۳

نیم سال تحصیلی: پاییز ۱۴۰۱

مدرّس: دکتر محمدحسین منشئی

۱

$m = (00110010)_2 = (50)_{10}$

$p = 23, q = 19$

$n = pq = 23 \times 19 = 437$

$z = (p-1)(q-1) = 22 \times 18 = 396$

$e = 97 \Rightarrow e < n,\ (e, z) = 1$

$d = 49 \Rightarrow ed \equiv 1 (mod\ z)$

$c = (m^e \equiv 1 (mod\ n)) \Rightarrow c = 335$

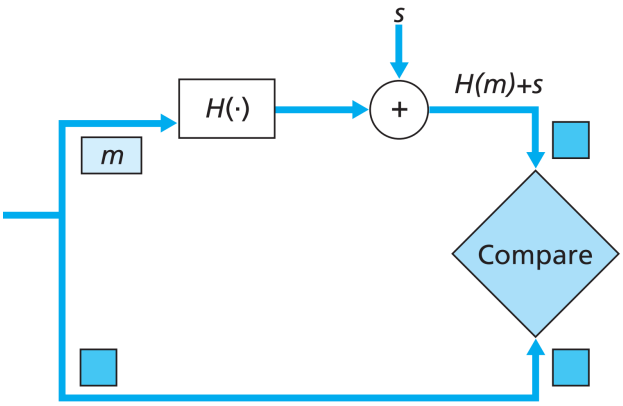
$m = (c^d \equiv 1 (mod\ n)) \Rightarrow m = 50$

$K^+ = e = 97$

$K^- = d = 49$

۲

Trudy می‌تواند به سیستم نفوذ کند و محتوای ارسال شده را تغییر دهد. به این صورت که M و $H(M) + S$ را از هم جدا می‌کند. سپس با محاسبه‌ی hash پیامِ M و حذف آن از $H(M) + S$ (به شکل $H(M) + S - H(M)$) به shared secret دست پیدا می‌کند. سپس پیام مورد نظر خود (M') را به همراه $H(M')$ و S برای فرد به شکل $(M', H(M') + S)$ ارسال می‌کند. با اینکه این پروتکل قابلیت نفوذ دارد اما به هر حال نمودار استخراج و Authenticationِ پیام به صورت زیر است.



شکل ۱: نمودار رمزگشایی پیام

۳

اول از هرچیز امضای message digest با کلید خصوصی (private key) صورت می‌گیرد، نه کلید عمومی (public key). به دلیل پیچیدگی محاسباتی عملیات رمزنگاری و رمزگشایی، کل پیام را رمز نمی‌کنیم و فقط digestش را رمز می‌کنیم.

۴

هزاران نفر قصد دارند پیام Alice را دریافت کنند و Alice آماده است که پیام را به هر متقاضی بفرستد. برای تضمین صحت پیام، Alice می‌تواند ابتدا hashِ پیام را با private keyِ خود رمز کند و همراه پیام $((m, K_A^-(H(m))))$ به هر یک از متقاضیان بفرستد. چون Alice تنها کسی است که private key خود را دارد و پیامی که با private key رمز شده است تنها با public key نظیر همان private key قابل رمزگشایی است، در این صورت هر یک از دریافت‌کننده‌های پیام می‌توانند صحت این پیام را احراز کنند. به این صورت که هر یک از دریافت‌کننده‌ها $K_A^-(H(m))$ و m را از هم جدا می‌کند. سپس با استفاده از public keyِ Alice $H(m)$ را به شکلِ $H(m) = K_A^+(K_A^-(H(m)))$ به دست می‌آورد. در نهایت با گرفتن hash از mِ جدا شده و بررسی برابریِ آن با $H(m)$ به دست آمده در مرحله‌ی قبل صحت پیام احراز می‌شود. توجه شود که برای دستیابی به صحت می‌توانستیم به جای مکانیزم امضای دیجیتال از MAC استفاده کنیم. اما در این حالت Alice باید به ازای هر دریافت‌کننده $(m, H(m + s))$ را محاسبه کند که خود این کار با توجه به تعداد زیاد دریافت‌کننده‌های پیام می‌تواند overhead قابل توجهی داشته باشد و همچنین لازم بود که به ازای هر دریافت‌کننده یک shared secret داشته باشد که مدیریت آن‌ها می‌تواند ساده نباشد.
پس در این جا استفاده از digital-signature-based integrity scheme نسبت به MAC algorithm scheme بهتر است.

۵

در اینجا Trudy نقش Man-in-the-middle را دارد و N_a و $E_k(N_b)$ و $E_k(N_a)$ و N_b را از طرف خود برای Bob و Alice می‌فرستد و به این صورت Authenticate می‌شود.

۶

الگوریتم SSL handshake به صورت زیر است.

۱. Bob لیستی از الگوریتم‌هایی که از آن‌ها پشتیبانی می‌کند را به همراه nonce به Alice می‌فرستد.

۲. Alice بین لیست الگوریتم‌های پیشنهادی یکی را انتخاب می‌کند و آن را به همراه certificate و nonce می‌فرستد.

۳. certificate Bob را اعتبارسنجی می‌کند، public keyِ Alice را استخراج می‌کند، pre_master_secret را تولید می‌کند، با public keyِ Alice آن را رمز می‌کند و برای Alice می‌فرستد.

۴. Bob و Alice به طور مستقل رمز و کلیدهای MAC را از pre_master_secret و nonceها محاسبه می‌کنند.

۵. Bob یک MAC از همه‌ی پیام‌های handshake می‌فرستد.

۶. Alice یک MAC از همه‌ی پیام‌های handshake می‌فرستد.

اگر Trudy خود را Alice جا زده باشد، در گام ۶ باید یک MAC ($H(m+s)$) از همه‌ی پیام‌های handshake به Bob بفرستد و از آن‌جایی که shared secret را ندارد نمی‌تواند MAC را به درستی محاسبه کند. پس Bob در ای ن گام متوجه می‌شود که با Alice در ارتباط نیست.

۷

فایروال‌های stateless پکت‌ها را به طور مستقل از یک دیگر در نظر می‌گیرند. در حالی که فایروال‌های stateful اطلاعات مربوط به پکت‌های قبلا منتقل شده را ذخیره می‌کنند. برای مثال حالتی که Attacker بدون آغاز کردن یک connection (که با Syn است) Ack می‌فرستد. اگر در این سمت یک فایروال stateful وجود داشته باشد این تغییر رفتاری را متوجه می‌شود. به طور کلی تفاوت فایروال stateless و stateful از قرار زیر است:

	Stateless Packet Filtering Firewalls	Stateful Packet Filtering Firewalls
1.	The stateless firewalls are designed to protect networks based on static information such as source and destination.	Stateful firewalls filter packets based on the full context of the connection.
2.	It uses some predefined packet filtering rules, the packets are judged based on that, if it conforms to the predefined rules then it is considered to be "safe" and allowed to pass through. If the conditions are not met, the packet is considered to be "unidentified" or "malicious" and it will be blocked.	It uses the concept of a state table where it stores the state of legitimate connections. Stateless firewall filters are only based on header information in a packet but stateful firewall filter inspects everything inside data packets, the characteristics of the data, and its channels of communication.
3.	Less secure than stateless firewalls.	Stateful firewalls are more secure.
4.	Cheaper or cost-efficient.	Expensive as compared to stateless firewall
5.	Faster than Stateful packet filtering firewall.	Slower in speed when compared to Stateless firewall.
6.	For small businesses, a stateless firewall could be a better option, as they face fewer threats and also have a limited budget in hand.	For larger enterprises, a stateful firewall would be a smarter option, as they have larger outgoing traffic that needs monitoring and enough money to afford it. Stateful firewalls offer dynamic packet filtering, so they can provide a thick security layer to mitigate attacks.

شکل ۲

۸

Attacker با IV شناخته شده به عنوان پایه شروع می‌کند و مکررا sub-attack را اعمال می‌کند تا همه‌ی کلیدواژه‌های در secret key را بازیابی کند. cryptoanalyst به اولین کلمه‌ی خروجی از تعداد زیادی RC4 stream به همراه IVای که برای تولید هر کدام از آن‌ها استفاده شده است نیاز دارد؛ و اولین کلمه‌ی پیام در اکثر پکت‌ها یک ثابت شناخته شده است. این الزامات به طور خودکار برآورده

می‌شوند.

با حدود ۶۰ IVای این‌چنینی، Attacker می‌تواند کلید را با احتمال موفقیت قابل قبول به دست آورد. تعداد پکت‌های مورد نیاز برای دستیابی به آن تعداد IV دقیقا به IVهایی که فرستنده استفاده می‌کند بستگی دارد. همچنین استاندارد 802.11b طریقه‌ی پیاده‌سازی این IVها را مشخص نکرده است. روش معمول استفاده از یک شمارش‌گر برای تولید آن‌هاست. اگر شمارش‌گر از ۰ شروع نشود، Attacker استراتژی مشابه دارد. اگر Attacker دو بایت اول secret key را در نظر بگیرد، برای هر بایت IV ابتدایی، تقریبا ۴ چینش از دو بایتی که جایگشت مورد نیاز برای بازیابی یک بایت شامل کلید را می‌سازد وجود دارد.

Fluhrer S.، Mantin I. و Shamir A. در Attacks on RC4 and WEP توضیح می‌دهند که x کلمه‌ی اول KSA key شناخته شده است. این قضیه باعث می‌شود که بتوان x دور اول KSA را شبیه‌سازی کنیم و جایگشت S_{x-1} و اندیس i_{x-1} در آن نقطه را محاسبه کنیم. مقدار بعدی i نیز شناخته شده است ($i_x = x$)، اما مقدار بعدی $j(j_x)$ به کلیدواژه‌ی هدف $K[x]$ وابسته است (چون $j_x = j_x - 1 + S_x - 1[x] + K[x]$) و در نتیجه هر یک از مقادیر j_x و $K[x]$ به سادگی از دیگری قابل بازیابی هستند. در نتیجه به ازای $S_x[x]$ داده شده می‌توان حساب کرد که کدام مقدار در جایگاه j_x در جایگشت شناخته شده‌ی S_{x-1} قرار داشته است و از طریق برعکس کردن این جایگشت می‌توان j_x را بازیابی کرد. برای توضیح بیشتر به منبع مراجعه کنید.

منابع

[1] Stošić, Lazar, and Milena Bogdanović. ”RC4 stream cipher and possible attacks on WEP.” Editorial Preface 3.3 (2012).