by : *الراشد* Created At: *2020-05-23 21:12:09*

رمزنگاری کلید عمومی یا نامتقارن

رمز نگاری کلید عمومی یا نامتقارن به انگلیسی asymmetric نوعی از رمز نگاری است که در آن برای رمز کردن اعداد از ۲ کلید به نام های کلید عمومی و خصوصی استفاده می‌کنیم؛ پیام های رمز شده با یک کلید, فقط با کلید دیگر قابل رمزگشایی هستند؛ از این ویژگی در امضای دیجیتال نیز استفاده می‌کنند.

این زوج کلید به صورت ۲ زوج مرتب مانند `{(d,n),(e,n)}` ارائه می‌شوند که d کلید خصوصی و e کلید عمومی و n نیز پیمانه رمزنگاری می‌باشد.

توابع

تابع ϕ یا φ

(http://hakanyurdakul.com/wp-content/uploads/totient.jpg)

تابع φ حساب می‌کند که تا نرسیده به عدد مورد نظر چند عدد نسبت به خود عدد متباین (coprime) هستند.

مثلا ۳ دارای ۲ عدد ۱ و ۲ به عنوان متباین تا نرسیده به خود است که φ(n) آن می‌شود ۲.

نکته: عدد ۱ نسبت به همه اعداد متباین است.

نکته: حاصل همه عبارات مقابل برابر است: `Lambda n` با `Phi n` با `LCM (Phi p , Phi q)` با `(p - 1) * (q - 1)` برابر است.

الگوریتم ها

Name	Developed At	Key Size
Eliptic Curve (EC)	-	256
Digital Signature Algorithm (DSA)	-	128
Rivest Shamir Adleman (RSA)	1977	3072

EC

درحال حاضر, الگوریتم, eliptic curve یا EC, با طول کلید کمتر, از RSA و DSA امن تر است.

RSA

ساخت کلید

برای ساخت زوج کلید عمومی و خصوصی به ترتیب زیر عمل می‌کنیم.

1. دو تصادفی و متفاوت اول به نام های p و q انتخاب کنید.
2. مقدار n را از حاصل ضرب p و q بدست آورید.

3. حاصل ϕ متغیر n را حساب کنید. λ یا ϕ متغیر n به عنوان پیمانه هم‌نهشت ها استفاده خواهد شد.

کلید عمومی یا e

کلید عمومی یا e عددی تصادفی بین $0 و ϕ(n) می‌باشد به طوری که **e و ϕ(n) نسبت بهم متباین باشند** یا به عبارت دیگر e مقسوم علیه یا مضرب مشترکی با ϕ متغیر n نداشته باشد.

- نکته: e در رمز نگاری های مواثر طول کمی دارد. متداول ترین عدد انتخاب شده عدد 65537 یا $2^{16}+1$ است که معادل باینری 10000000000000001 می‌باشد, و کوچک ترین عدد ممکن ۳ می‌باشد.
- نکته: علت اینکه e عددی بین ۱ و پیمانه است, این است که اگر صفر باشد, اصلا نمی‌توان عدد را رمز کرد, و اگر بیشتر از پیمانه باشد, تکرار بی‌خود داشته ایم.

کلید خصوصی یا d

کلید خصوصی از معادله `ed≡1 mod phi(n)` بدست می‌آید؛ به این نوع هم‌نهشت, هم‌نهشت هماهنگ می‌گویند؛ توجه شود که d قرار نیست معکوس e باشد؛ یعنی اگر پیمانه ۱۰ بود, با تولید ۱۱ می‌توان به ۱ رسید.

- نکته: کلید عمومی (e) هیچ گاه با کلید خصوصی یا d برابر نیست.
- نکته: انتخاب کلید عمومی بزرگ یا e بزرگ باعث کاهش مقدار کلید خصوصی یا d می‌شود, و این مسئله از نظر امنیتی, رمز نگاری را در مقابل حملاتی همچون wiener's attack آسیب پذیر می‌کند.

رمزنگاری و باز کردن

رمزنگاری, یک پروسه محاسبه ریاضی است؛ بنابر این, ابتدا باید پیام را به بلوک های K کاراکتری یا K بایتی تبدیل کنیم, و هر بلوک را طبق قاعده‌ای کاملاً دلخواه به یک عدد صحیح به نام Pi تبدیل کنیم.

رمز کردن

با جفت عدد `(k,n)` به ازای یکایک بلوکهای Pi, اعداد جدیدی طبق رابطه `(Pi)(Key) mod ϕ(n)` بدست می‌آوریم که پیام را رمز می‌کند.

از رمز خارج کردن

پیام رمز شده را با کلید مخالف از حالت رمز خارج می‌کنیم.

- اگر با کلید عمومی پیام را رمز کرده باشیم, جفت عدد از رمز خارج کردن: `(d,n)` است
- اگر با کلید خصوصی پیام را رمز کرده باشیم, جفت عدد از رمز خارج کردن: `(e,n)` است.

با رابطه `(Pi)(Key) mod ϕ(n)` پیام اصلی را بدست می‌آوریم و همانطور که پیام را به عدد تبدیل کرده بودیم, دوباره به متن تبدیل می‌کنیم.

بازکردن

مثال ها

برای فهم بهتر, چند مثال عملی از رمزنگاری کلید عمومی یا نا متقارن در زیر آورده شده است.

مثال یکم RSA

اعداد p و q را به ترتیب ۵ و ۷ انتخاب می‌کنیم که n برابر خواهد بود با ۳۵. حاصل فی n را بدست می‌آوریم که می‌شود ۲۴. کلید عمومی را عددی بین ۱ و ϕ متغیر n انتخاب می‌کنیم که شمارنده مشترکی با فی n نداشته باشد. در اینجا ۲۳ می‌گیریم بود. طبق معادله یک کلید خصوصی انتخاب می‌کنیم. در اینجا کلید خصوصی و عمومی یکسان خواهند بود.

اثبات: پیام فرضی را ۲ در نظر می‌گیریم. پیام رمز شده برابر خواهد بود با (۲۳)(۲) پیمانه ۲۴ که حاصل ۲۲ است و پیام خارج شده از رمز هم برابر خواهد بود با (۲۳)(۲۲) با همنهشت ۲۴ که حاصل همان ورودی یعنی ۲ خواهد بود.

مثال دوم RSA

۲ عدد اول را ۲ و ۵ انتخاب می‌کنیم. حاصل ضرب آنهارا بدست می‌آوریم که ۱۰ است. پیمانه را حساب می‌کنیم که می‌شود ۱,۳,۷,۹ که برابر ۴ است. کلید عمومی را بدست می‌آوریم که در اینجا ۳ می‌گیریم (چیز دیگری هم نمی‌تواند باشد). کلید خصوصی نیز طبق معادله می‌تواند اعداد ۳ و ۷ و غیره باشد که ما ۷ را انتخاب می‌کنیم.

اثبات: متن را 3 میگیریم. اگر با کلید عمومی پیام را رمز کنیم خواهیم داشت (۳)(۳) با پیمانه ۴ که خواهد داد ۱. برای خارج کردن از حالت رمز هم (۷)(۱) با پیمانه ۴ داریم که حاصل همان ۳ خواهد بود.

نکته اساسی در RSA آن است که جهت تضمین وارون پذیری روش رمز، اعداد و بایستی در رابطه زیر صدق کنند.

$$ed \equiv 1 \bmod (\phi(n)) \Rightarrow ed(x) \equiv x \bmod (\phi(n))$$

در کاربردهای عملی، اعداد p و q حداقل صد رقمی (صد رقم در مبنای ده) انتخاب می شوند یعنی این دو عدد حداقل از مرتبه ۱۰۱۰۰ هستند.

پیوند ها

- RSA Algorithm
- Simple RSA key generation
- Why is a smaller value preferred for the public key in rsa
- In RSA, why is it important to choose e so that it is coprime to φ(n)?
- How do I find D in RSA?

Related posts

- رمز، رمزه و پاد رمزه چه هستند
- آموزش کانفیگ و اجرای پروتوکل SSL با openSSL
- کاربرد nonce در رمزنگاری چیست
- آموزش tmux و کانفیگ آن
- آموزش باز کردن قفل به روش پایه بردای یا lock picking

Updated At: 2026-05-04 05:16:35

username: x4748@tridectet.ir