CRIPTOGRAFIA DE CHAVE PÚBLICA: CURVAS ELÍPTICAS E RSA

RESUMO. A criptografia é a ciência que estuda as possíveis transformações de uma mensagem para que, quando transmitida por um canal inseguro, só possa ser interpretada pelo destinatário. A criptografia, que existe desde que existem segredos, não é mais para uso exclusivo de governantes ou militares. Hoje a criptografia faz parte do nosso dia a dia. Foi o uso de computadores e o nascimento das primeiras redes que impulsionaram a extraordinária expansão dos métodos criptográficos nos últimos 40 anos. Toda vez que fazemos compras online ou utilizamos nosso certificado digital para realizar um procedimento administrativo, estamos usando métodos criptográficos. Nosso dinheiro ou a confidencialidade de nossos dados pessoais dependem de que todos os processos envolvidos sejam suficientemente seguros. O objetivo do projeto é fazer uma aproximação aos principais algoritmos criptográficos utilizados atualmente, com foco nos algoritmos assimétricos, mais especificamente o RSA, suas fraquezas e as curvas elípticas.

O projeto constará de três etapas: uma primeira etapa de estudo introdutório sobre criptografia geral, uma segunda etapa sobre o estudo de criptografia assimétrica e uma última etapa com foco especial no RSA, suas fraquezas, algoritmos de fatoração e curvas elípticas como alternativa ao RSA. Também revisaremos brevemente o conceito de assinatura digital e alguns algoritmos de assinatura digital baseados em criptografia assimétrica.

SUMÁRIO

1. PROJETO

1.1. **Introdução à criptografia.** A primeira etapa consistirá basicamente em um estudo introdutório dos principais conceitos da criptografia através do estudo de textos clássicos da área, entre

os quais citamos [1] e [2], e algumas referências mais atuais [3, 4]. O objetivo é introduzir e consolidar os conceitos básicos. A estudante estudará de modo autônomo e apresentará os conteúdos na forma de seminários semanais, de modo que cobrirá os conteúdos de um curso de nível iniciante de Introdução à Criptografia. Todos os seminários serão supervisados pela orientadora e servirão para resolver eventuais dúvidas.

Os principais tópicos a serem abordados nesta primeira etapa são os seguintes:

(1) Arimética modular
(2) Conceitos de anel e corpo
(3) Arimética binária
(4) Diferenças entre criptografia simétrica e assimétrica
(5) Diferenças entre cifradores de bloco e cifradores de fluxo
(6) Algoritmos de bloco: DES, AES

1.2. **Criptografia assimétrica.** Na criptografia simétrica, uma única chave é usada para cifrar e decifrar. Ambas as partes da comunicação devem compartilhar esta chave através de um canal seguro antes de se comunicar. Na criptografia assimétrica (ou de chave pública) a troca de mensagens se realiza sem ter acordado uma chave secreta previamente. Nos algoritmos assimétricos, existem duas chaves, uma pública e uma privada. A chave pública é conhecida por todos e é usada para cifrar, Por sua vez, a chave privada é usada para decifrar. Qualquer pessoa que conheça a chave pública pode cifrar mensagens, porém apenas quem conhece a privada pode recuperar a informação.

A ideia original é atribuída a Whitfield Diffie e Martin Hellman. Em [5], eles propuseram um protocolo de troca de chave através de um canal inseguro usando apenas chaves públicas, ou seja, sem ter acordado uma chave privada antes. A segurança deste algoritmo está baseada no problema do logaritmo discreto, o qual descrevemos a continuação. Seja $\mathbb{F}_p$ o corpo de Galois de p elementos, p primo, e α um elemento primitivo. Dado $\alpha^t \bmod p$, com α e p conhecidos, então o problema do logaritmo discreto consiste em determinar o exponente t (vide [1] para mais detalhes). Quando p é grande (1024 bits ou mais), é computacionalmente impossível recuperar t.

Além do protocolo Diffie-Hellman, na atualidade existem diversos algoritmos assimétricos conhecidos. Por exemplo, os mais usados hoje em dia são o RSA e as curvas elípticas. O objetivo desta etapa é estudar estes algoritmos e entender as características deste tipo de criptografia.

1.3. **RSA.** O acrônimo RSA é composto das letras iniciais dos sobrenomes dos criadores de tal algoritmo, Ron Rivest, Adi Shamir e Leonard Adleman. Assumamos que Alice quer mandar uma mensagem a Bob. Bob cria e publica uma chave pública baseada no produto de dois números primos grandes (secretos), junto com um valor auxiliar. Alice (ou qualquer pessoa) pode usar a chave pública para cifrar a mensagem, mas apenas Bob que conhece a chave privada (os dois primos) pode decifrar a mensagem. A segurança do RSA é baseada na dificuldade prática da fatoração do produto de dois números primos grandes.

O RSA (e qualquer algoritmo assimétrico em geral) é um algoritmo relativamente lento. Portanto ele é usado normalmente para compartilhar chaves curtas simétricas, dado que os algoritmos simétricos são em geral mais rápidos.

A fatoração do produto de primos grandes é um problema aberto. No entanto, existem algumas recomendações em relação à escolha destes primos: eles devem ter o mesmo comprimento (em bits), não devem ficar muito próximos, devem ser primos “fortes”, etc.

O objetivo principal desta etapa é conhecer com profundidade o algoritmo RSA e as possíveis fraquezas [6, 7, 8]. Além disso, é conveniente estudar os algoritmos de fatoração conhecidos atualmente [9, 10, 11, 12].

1.4. **Curvas elípticas.** Uma curva elíptica sobre $\mathbb{Z}_p$, $p > 3$, é o conjunto dos pares (x, y), $x, y \in \mathbb{Z}_p$, que satisfazem

$$y^2 \equiv x^3 + ax + b \bmod p, \quad a, b \in \mathbb{Z}_p$$

junto com um ponto imaginário chamado ponto no infinito $\mathcal{O}$ e $4a^3 + 27b^2 \not\equiv 0 \bmod p$.

Queremos definir um grupo cíclico usando os pontos da curva elíptica, portanto precisamos de uma operação. Dados dois pontos da curva $P = (x_1, y_1), Q = (x_2, y_2) \in \mathcal{E}$, definimos a soma entre eles como outro ponto da curva $R = P + Q = (x_3, y_3)$ tal que

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \bmod p, \\ y_3 &= m(x_1 - x_3) - y_1 \bmod p, \end{aligned}$$

para

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p \text{ se } P \neq Q, \\ \frac{3x_1^2 + a}{2y_1} \bmod p \text{ se } P = Q, \end{cases}$$

onde m é o coeficiente angular da reta definida por P e Q. O elemento neutro deve ser um ponto $\mathcal{O}$ tal que $P + \mathcal{O} = P$ e se $P = (x, y)$ então $-P = (x, -y)$ ($-y \bmod p$).

Os pontos de uma curva elíptica junto com $\mathcal{O}$ e a operação definida acima tem subgrupos cíclicos. Sob certas condições, todos os pontos formam um grupo cíclico [1]. Neste caso, podemos definir o problema do logaritmo discreto sobre este grupo igual que acontecia com $(\mathbb{F}_p, *)$. Dada uma curva elíptica $\mathcal{E}$, P um elemento primitivo e T um elemento da curva, o problema do logaritmo discreto é encontrar um d inteiro, $1 \leq d \leq |\mathcal{E}|$ tal que $\underbrace{P + P + \cdots + P}_{d \text{ vezes}} = dP = T$. Como consequência, é possível definir um protocolo de troca de chave similar ao de Diffie-Hellman usando curvas elípticas [1].

O objetivo desta etapa do projeto é entender as características das curvas elípticas e as possíveis aplicações destas curvas à criptografia. Além disso, é conveniente estudar as vantagens e desvantagens de usar curvas elípticas em vez de RSA.

1.5. **Assinatura digital.** Assumamos que Alice quer mandar uma mensagem x para Bob e quer assinar essa mensagem para provar que foi ela que mandou. Para isso, ela vai usar uma assinatura digital, i.e., uma função da mensagem x e a chave privada k: $y = sign_k(x)$. Depois de criar a assinatura, ela vai mandar a mensagem junto com a assinatura, (x, y), através do canal Para verificar se foi Alice quem realmente mandou a mensagem, Bob usa uma função de verificação usando a mesma chave privada k: $ver_k(y)$. Ele confere se o resultado de $ver_k(y)$ coincide com x. Se for assim, então sabe que foi Alice que mandou a mensagem e a mensagem não sofreu nenhuma alteração dentro do canal, se não então ele sabe que teve algum ataque ou interferência e pode pedir para ela mandar de novo. Note-se que ambas as partes conhecem a chave secreta. Para mais informações, consultar [13].

A assinatura digital não fornece confidencialidade, pois não cifra a mensagem, porém proporciona integridade e autenticidade. No caso de usar a mesma chave, a assinatura digital não fornece não repúdio, dado que a parte assinante pode alegar que a outra parte que falseou a assinatura. Para conseguir não repúdio precisamos de criptografia assimétrica. Existem vários algoritmos de assinatura digital que usam criptografia de chave pública, por exemplo, existem algoritmos de assinatura digital baseados em RSA, ElGamal, DSA, Rabin ou Curvas Elípticas [1].

Aqui, pretendemos estudar o conceito e as propriedades das assinaturas digitais e estudar algumas das assinaturas derivadas dos algoritmos assimétricos mais conhecidos.

2. Objetivos

- Conhecer a diferença entre criptografia simétrica e assimétrica.
- Conhecer os principais algoritmos criptográficos conhecidos na atualidade.
- Conhecer os diferentes algoritmos assimétricos e saber implementá-los.
- Estudar e conhecer as aplicações das curvas elípticas em criptografia.
- Conhecer as vulnerabilidades do RSA.
- Estudar o conceito de assinatura digital e algumas assinaturas derivadas de algoritmos assimétricos.

3. Cronograma

- Etapa I: Quatro meses de estudos introdutórios orientados. Estudo dos tópicos básicos de criptografia e a matemática necessária (aritmética modular, aritmética binária, corpos e anéis) através das referências clássicas [1, 2] e outras. Esta etapa é equivalente ao estudo de uma disciplina de Introdução à Criptografia.
- Etapa II: Consistirá em 2 messes de estudo dos algoritmos de criptografia assimétrica mais conhecidos: RSA, ElGamal, Rabin, etc.
- Etapa III: Dois meses de estudo das fraquezas do RSA e algoritmos de fatoração.
- Etapa IV: Dois meses de estudo de curvas elípticas e aplicações básicas à criptografia.
- Etapa V: Dois meses de estudo do conceito assinatura digital e as possíveis assinaturas derivadas dos algoritmos de criptografia pública vistos anteriormente.

4. Atividades previstas

- Participação no Simpósio de Iniciação Científica da UFABC de 2023.
- Participação em seminários e palestras relacionados com a área.

5. Metodologia

- Reuniões semanais com a orientadora para apresentar os conceitos aprendidos em forma de seminário.
- Estudo dos conceitos necessários através das referências recomendadas pela orientadora.
- Visualização de vídeo-aulas sobre Introdução à criptografia como complemento ao material escrito.
- Realização de relatórios parciais a cada três meses, os quais englobarão os conceitos aprendidos até o momento.

Referências

[1] C. Paar and J. Pelzl, *Understanding Cryptography*. Berlin: Springer, 2010.
[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1996.
[3] N. P. Smart, *Cryptography Made Simple*, 1st ed. Springer Publishing Company, Incorporated, 2015.
[4] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed. Chapman & Hall/CRC, 2020.
[5] W. D. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[6] M. Bakhtiari and M. A. B. Maarof, "Serious security weakness in RSA cryptosystem," 2012.
[7] I. Blagoev, T. Balabanov, and I. Iliev, "RSA weaknesses caused by the specifics of random number generation," *Information & Security: An International Journal*, vol. 50, no. 2, pp. 171–179, 2021.
[8] K. Somsuk, "The new weakness of RSA and the algorithm to solve this problem," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 9, pp. 3841–3857, September 2020.

[9] D. M. Bressoud, *Factorization and Primality Testing*. New York: Springer-Verlag, 1989.
[10] L. E. Dickson, "Methods of factoring," in *History of the Theory of Numbers, Volume I: Divisibility and Primality*. Dover, 2012, ch. 14, pp. 357–374.
[11] A. Overmars and S. Venkatraman, "New semi-prime factorization and application in large RSA key attacks," *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 660–674, 2021.
[12] B. Wang, F. Hu, H. Yao, and C. Wang, "Prime factorization algorithm based on parameter optimization of Ising model," *Scientific Reports*, vol. 10, pp. 1–10, 2020.
[13] J. Katz, *Digital Signatures*. New York: Springer, 2010.