Universidade: presente!

UFRGS PROPESQ

XXXI SIC

Salão UFRGS 2019 — Conhecimento o Formação o Inovação

21 . 25 . OUTUBRO . CAMPUS DO VALE

Sistema de Criptografia de ElGamal

Cibele da Rocha Schmitz

Orientadora: Juliane Golubinski Capaverde

Introdução

Em 1985 Taher ElGamal introduziu um método de encriptação de mensagens baseado no problema do logaritmo discreto. Este sistema de criptografia é do tipo assimétrico, que é muito utilizada para proteção de dados que trafegam em meios públicos.

Nos sistemas assimétricos, é utilizada uma chave (pública) para encriptar mensagens e outra (privada) para decriptá-las. A ideia é que qualquer usuário pode encriptar mensagens utilizando a chave pública, mas somente o destinatário pretendido, que possui a chave privada, será capaz de decriptá-las.

Por exemplo, se Alice quer enviar uma mensagem de forma segura para Bob, em que somente ele consiga lê-la, ela deve encriptar a mensagem utilizando a chave pública dele. Somente Bob tem acesso à sua chave privada, portanto, ele é o único capaz de decriptar a mensagem de volta para sua forma original. Mesmo que alguém tenha acesso a mensagem criptografada, a mesma vai permanecer confidencial, já que nenhuma outra pessoa além de Bob pode decifrar a mensagem.

A seguir, descrevemos como são feitas a geração das chaves pública e privada, a encriptação e a decriptação no sistema ElGamal.

Geração de Chaves

Para criar o sistema de criptografia a ser utilizado na comunicação, um usuário, que será o receptor das mensagens, deverá seguir os seguintes passos:

- Escolher um primo grande p;
- Escolher uma raiz primitiva r deste primo;
- Escolher um número natural $2 < x \leq p-2$ aleatoriamente;
- Calcular $r^x \equiv a \pmod{p}$;
- Divulgar sua chave pública (p, r, a);
- Manter sua chave privada x em segredo.

Por exemplo, digamos que Alice e Bob queiram se comunicar de forma segura. Bob então escolhe $p = 1009$, $r = 11$ e $x = 13$. Ele calcula $11^{13} \equiv 752 \pmod{1009}$ e divulga a chave pública $(1009, 11, 752)$, mantendo x em segredo.

Encriptação

A fim de cifrar a mensagem, o emissor deve, primeiramente, convertê-la em uma sequência de dígitos, formando um número K. Isso deve ser feito de uma forma convencionada, por exemplo, fazendo a substituição $A = 00, B = 01, ..., Z = 25$. Se $K \geq p$, a mensagem deve ser dividida em blocos, de maneira que cada bloco seja menor ou igual a $p-1$. Cada bloco M é então encriptado separadamente, da seguinte forma:

- Obter a chave pública (p, r, a) do receptor;
- Escolher um número natural $2 < y \leq p-2$ aleatoriamente;
- Calcular $r^y \equiv b \pmod{p}$;
- Calcular $C \equiv M.a^y \pmod{p}$;
- Enviar o ciframento $c = (b, C)$.

Suponhamos que Alice deseja enviar mensagem $K = 281813$ a Bob. Ela primeiro vai dividir a mensagem nos blocos 281 e 813. Para encriptar o primeiro bloco $M = 281$, ela escolhe $y = 69$, e calcula $b \equiv 11^{69} \equiv 899 \pmod{1009}$ e $C \equiv 281.752^{69} \equiv 281.371 \equiv 324 \pmod{1009}$. Alice então envia a mensagem cifrada $c = (899, 324)$, e repete o processo para o segundo bloco 813.

Decriptação

Para decifrar a mensagem $c = (b, C)$ recebida, o receptor deverá:

- Utilizar a chave privada para calcular $P \equiv C.b^{p-1-x} \pmod{p}$
- Temos que $C \equiv M.a^y \pmod{p}$ e que $b \equiv r^y \pmod{p}$, então:

$$P \equiv (M.a^y)(r^y)^{p-1-x} \equiv M(r^x)^y(r^{y(p-1)-xy}) \equiv M(r^{p-1})^y \equiv M \pmod{p}.$$

Ao receber a mensagem cifrada $c = (899, 324)$, Bob calculará $P \equiv 324.899^{1009-1-13} \equiv 324.359 \equiv 281 \pmod{1009}$, recuperando assim a mensagem original $281 = M$.

Segurança

Uma terceira pessoa que intercepte a mensagem terá conhecimento de p, r, a, b e C, mas não de x e y. Para decriptar a mensagem, a pessoa teria que resolver $r^x \equiv a \pmod{p}$ para x, ou $r^y \equiv b \pmod{p}$ para y. Resolver uma dessas congruências significa resolver um problema do logaritmo discreto, o que é computacionalmente difícil se p é um número primo muito grande (geralmente no mínimo 1024-bit ≈ 309 dígitos) e tal que $p-1$ tem um fator primo grande. Outro fator de segurança é a aleatoriedade na escolha das chaves privadas, o que evita ataques por análises estatísticas.

Referências

BURTON, David M. Elementary Number Theory.

DONG, Changyu. Math in Network Security: A Crash Course