Instituto Tecnológico de Aeronáutica
Curso de Engenharia da Computação
Disciplina de CTC-21

Sistema criptográfico em RSA

Dylan Nakandakari Sugimoto
Gabriel Adriano de Melo
Laurival Siqueira Calçada Neto
Thiago Filipe de Medeiros

PROJETO DE PESQUISA

Docente: Carlos Ribeiro

São José dos Campos
MAIO / 2017

Motivação

Nas últimas décadas, a crescente evolução tecnológica mudou completamente o estilo de vida das pessoas: o surgimento da internet e da comunicação celular facilitou a integração social; a capacidade de lançar satélites para monitoramento facilitou a localização e tornou mais sensível as relações políticas pelo mundo; a automação na indústrial substituiu as pessoas em trabalhos repetitivos que demandavam um alto esforço físico e psicológico e forçou a sociedade a se tornar mais capacitada para suprir os serviços que as máquinas ainda não podem realizar; o desenvolvimento de ferramentas, aliada ao esforço intelectual, possibilitou a realização de projetos que mais parecem saídos de filmes de ficção científica, como inteligências artificiais e robôs para o auxílio em resgates e salvamentos.

Nesta era de informação, a humanidade está se tornando cada vez mais dependente dos bits, chips, processadores e antenas. Contudo, há um ponto fraco da dependência dos circuitos que já foi exposto diversas vezes: a segurança.

A possibilidade de interceptação indesejada e/ou exposição de informações é extremamente preocupante em um mundo que, cada vez mais, se apoia na tecnologia. Neste panorama, a criptografia RSA se destaca por possibilitar a comunicação segura de informações em um ambiente inseguro e, até então, ter resistido a todas as tentativas de quebra. Esse é o principal método de criptografia utilizado na segurança de informações trocadas via internet. Devido à sua base na Teoria dos Números, que está inserida no contexto da matemática discreta, conteúdo ministrado na disciplina CTC21, este tema foi escolhido para o trabalho solicitado.

Metodologia

O projeto será executado em três etapas:

- Busca por informações no sentido de compreender o funcionamento do método de criptografia RSA e a sua relação com a disciplina CTC-21.

- Tentativa de implementar o método em código utilizando as linguagens recomendadas, documentando o código à medida que ele for escrito.

- Analisar o código e escrever o relatório.

Para isso o grupo cogita utilizar as seguintes ferramentas de pesquisa:

- Consulta a livros;

- Pesquisa na internet;

- Consulta a artigos científicos relacionados ao assunto;

- Consulta a tutoriais relacionados ao assunto;
- Consulta a fóruns relacionados ao assunto;
- Consulta a professores da área de criptografia para retirar possíveis dúvidas.