Em 1978, R. L. Rivest, A. Shamir e L. Adleman inventaram o sistema de criptografia RSA. Desde então, tal método se tornou o mais usado em aplicações comerciais. Com isso, muitos ficaram sabendo da existência do RSA. Porém, nem todos sabem, de fato, em que consiste tal método.

Além disso, uma questão que é extremamente pertinente a esse tema é a seguinte: por que o método RSA é tão seguro? A resposta a essa pergunta está relacionada com o conceito de "sistemas de criptografia de chave pública" e com o problema da fatoração nos inteiros.

Na apresentação deste trabalho, eu irei prover uma explicação sucinta do RSA, e depois irei me concentrar em um aspecto específico do método, analisando algumas questões referentes a sua segurança.