EFFICIENT VARIANT OF RSA

CC1501 PROJECT PRESENTATION

PRESENTED BY KARTIK SINGHAL AND KARTHIK AGARWAL

CONTENTS

INTRODUCTION

We implement and analyze the standard RSA algorithm, understanding its deficiency and to further optimize it through designing and combining the RSA algorithm with Chinese Remainder Theorem to speed up RSA decryption by an approximate **factor of four.**

RSA

RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

HOW RSA WORKS?

RSA Algorithm

Key Generation

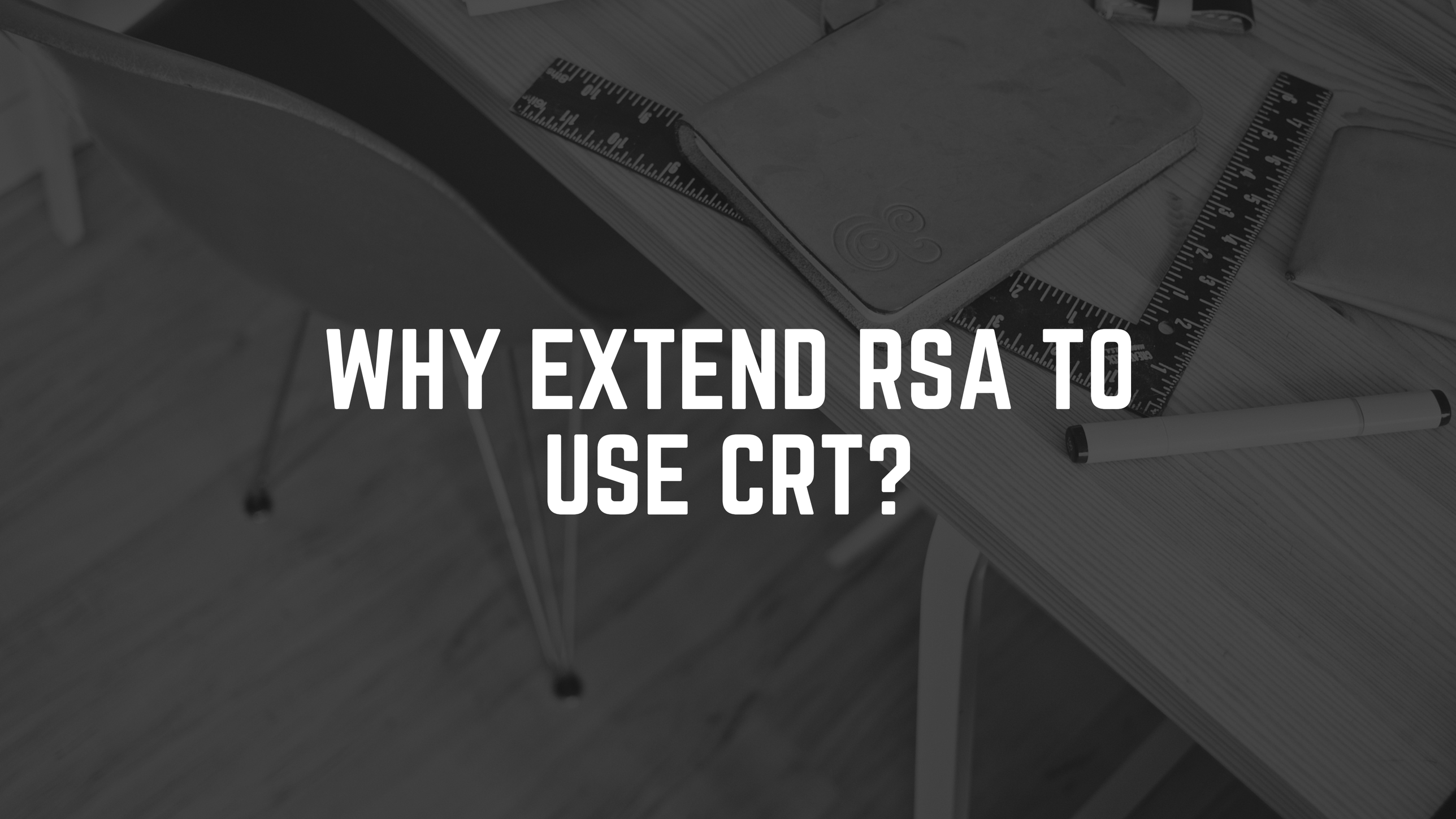
Select p,q	p and q both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e,n\}$
Private key	$KR = \{d,n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Plaintext:	C
Ciphertext:	$M = C^d \pmod n$



WHY EXTEND RSA TO USE CRT?

PROBLEM

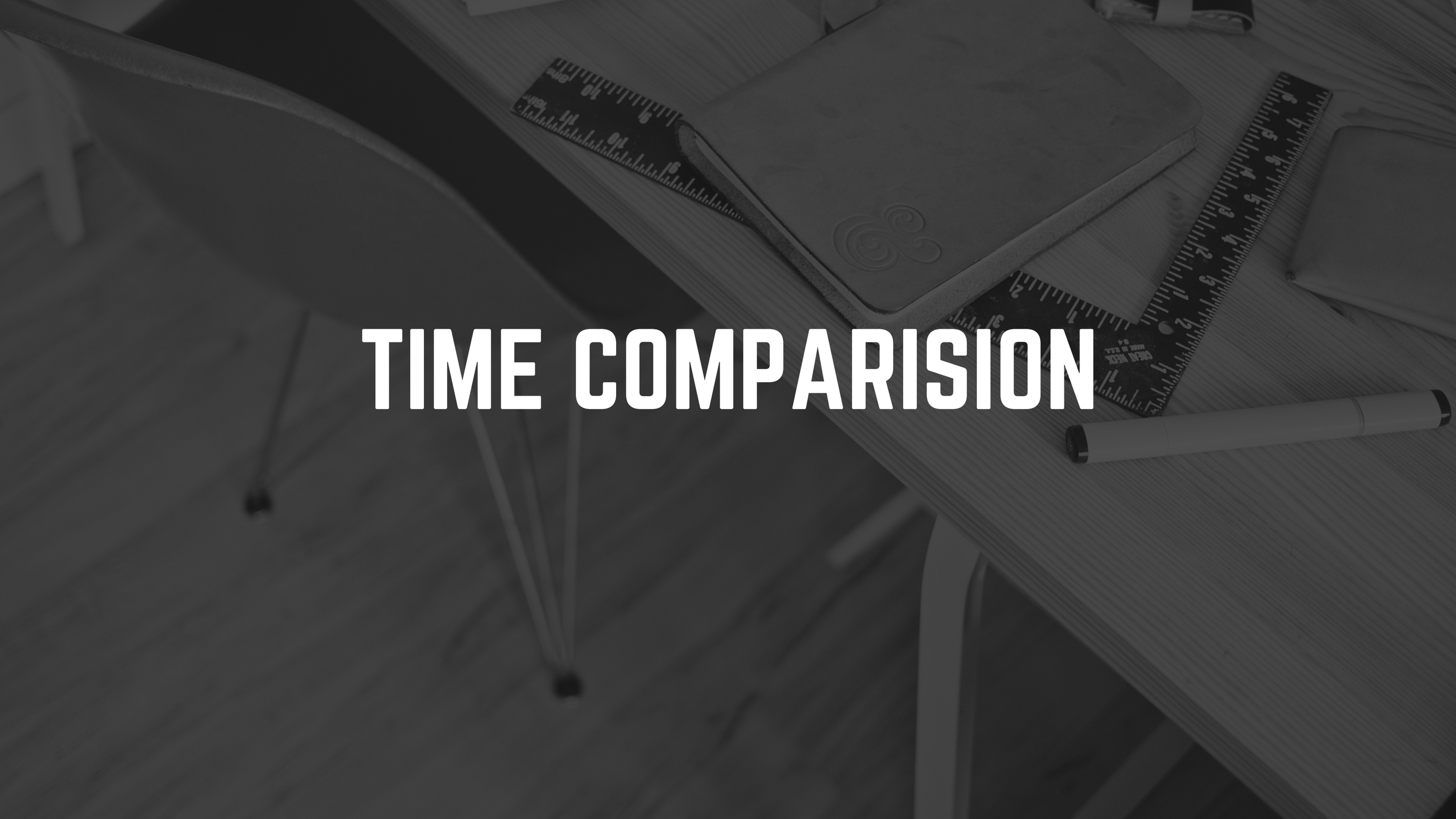
RSA encryption and decryption algorithm needs a lot of calculation and the speed is slow, and because of this, it is less commonly used to directly encrypt user data. More often, RSA encrypts shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed. Therefore, there was a need to make RSA work faster through CRT and other means.

- p and q: the primes from the key generation,
- $d_P = d \pmod{p-1}$,
- $d_Q = d \pmod{q-1}$ and
- $q_{\text{inv}} = q^{-1} \pmod{p}$.

- $m_1 = c^{d_P} \pmod{p}$
- $m_2 = c^{d_Q} \pmod{q}$
- $h = q_{\text{inv}}(m_1 - m_2) \pmod{p}$
- $m = m_2 + hq$

WHY CRT IS FASTER

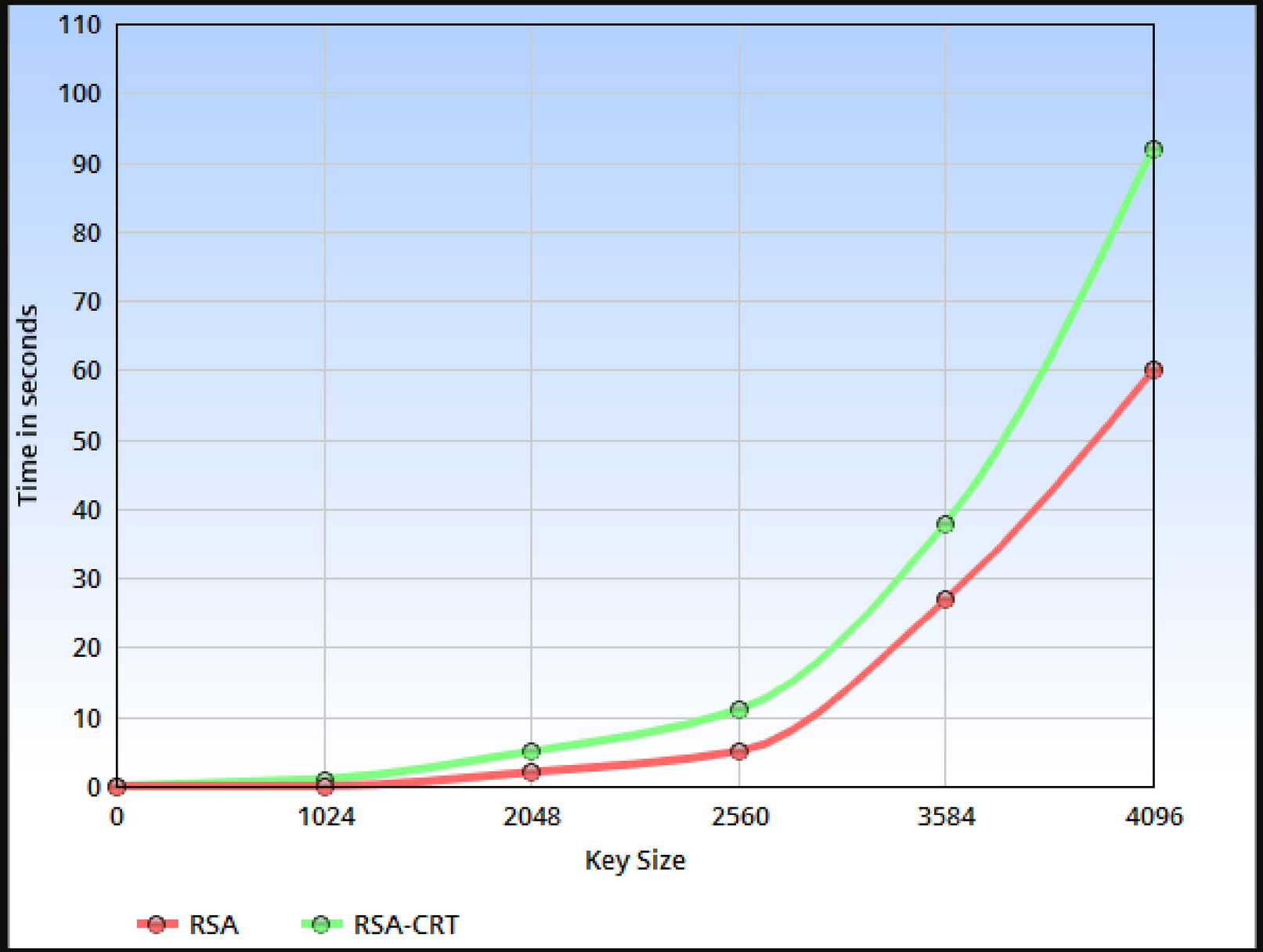
This is more efficient than computing square curve exponentiation even though two modular exponentiations have to be computed. The reason is that these two modular exponentiations both use a smaller exponent and a smaller modulus.



TIME COMPARISION

DECRYPTION TIME

KEY GENERATION TIME



THANK YOU

KARTHIK AGARWAL
KARTIK SINGHAL