

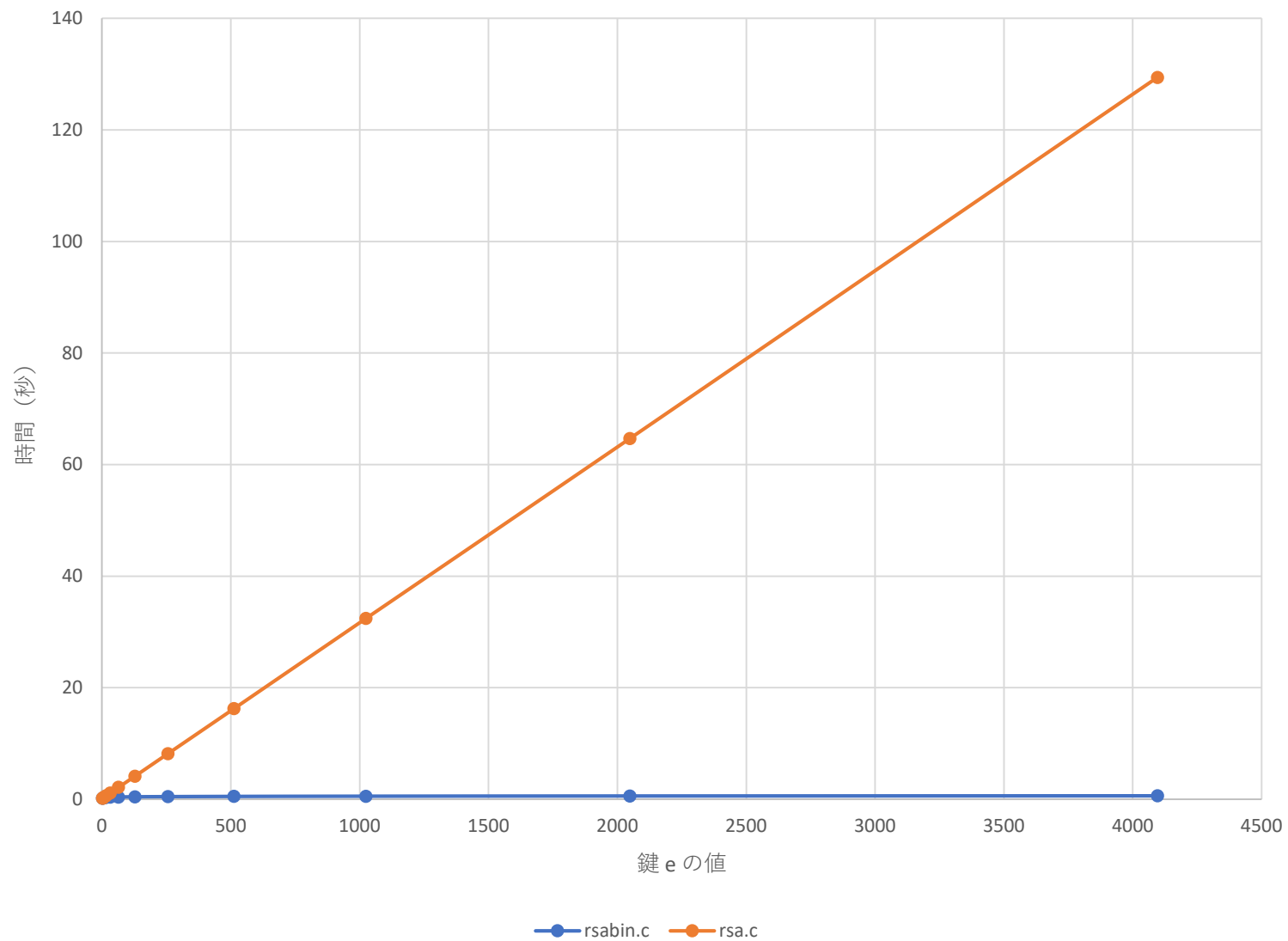
プログラム rsabin.c と rsa.c の平均実行処理時間について

- 比較対象の2種類のプログラム：
 - rsa.c (RSA 暗号のプログラム)
 - rsabin.c (2 進展開法を用いた RSA 暗号のプログラム)
- 実装に用いた計算機: Sun Microsystems sun4v T5440(Frequency: 1414 MHz)
- 実装に用いたファイルサイズ: 509.821Kbytes
- 各鍵 e の整数値に対し、10 回の試行実験をした平均実行処理時間を以下の表に示す。単位は秒である。グラフは次ページ以降に示すが、エクセルを用いて作成した。

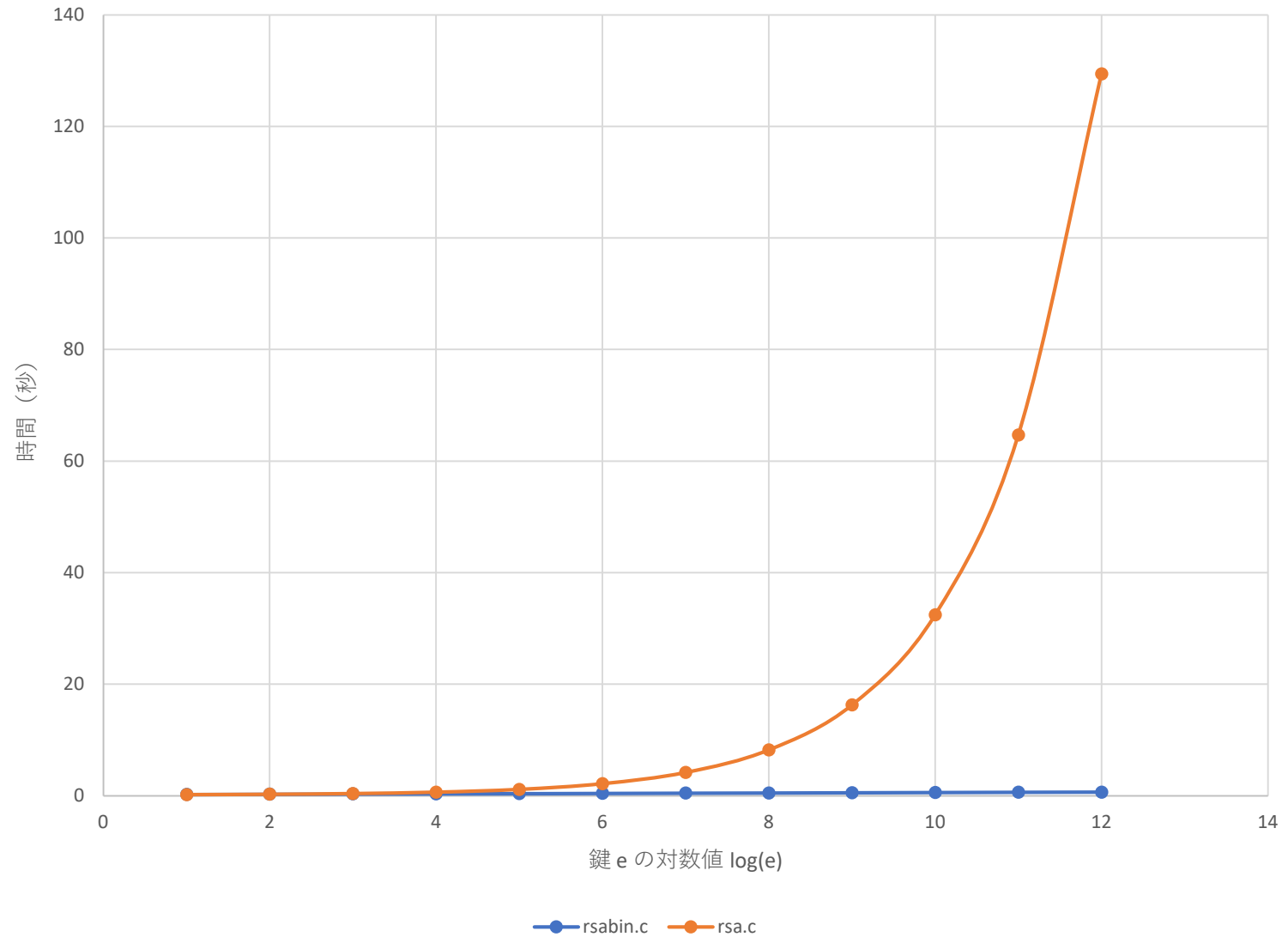
e	2	4	8	16	32	64	128	256	512	1024	2048	4096
log(e)	1	2	3	4	5	6	7	8	9	10	11	12
rsabin.c	0.23	0.27	0.31	0.35	0.38	0.42	0.46	0.49	0.53	0.57	0.61	0.64
rsa.c	0.2	0.26	0.39	0.64	1.14	2.16	4.17	8.21	16.27	32.43	64.67	129.42

- 2つのプログラムの実行処理時間のデータを表とグラフにして表す意図のひとつとして、アルゴリズムの理論における時間計算量と実際の処理時間が妥当であるかを確認することがある。
- 実測した処理時間が鍵の値に対し、線形関数として変化するのか、対数関数として変化するのかを確認すること。

rsa.cとrsabin.cの実行処理時間の比較



rsa.cとrsabin.cの実行処理時間の比較（横軸：e の対数値（対数の底 2））



2進展法を用いたrsabin.cの実行処理時間と対数 $0.06 * \log(e)$ との比較 (対数の底 2)

