



APPLICATION NOTE 4004

RSA Key Generation in DS5250

Abstract: The DS5250 microcontroller evaluation (EV) kit is a proven platform to evaluate the capabilities of this high-speed secure microcontroller. This application note demonstrates how to setup the EV kit and generate the RSA key-pair of the bit length needed for an application. The Keil μ Vision2[®] compiler is used to develop the library and sample application. The Microcontroller Tool Kit (MTK) is used to load the application on the EV kit and to observe the results.

Introduction

This application note describes how to setup the [DS5250](#) secure microcontroller's evaluation (EV) kit. (Contact micro.support@maxim-ic.com for information on purchasing this EV kit.) The article explains how to generate the RSA key-pair sets using the library provided for the microcontroller.

The EV kit contains the DS5250 microprocessor, 1MB of battery-backed SRAM, 1MB Flash memory, a power-supply regulator, two DB-9 serial connectors, and switches and LEDs to control and display board operation. By adding a power supply and an RS-232 cable connected to a personal computer, the kit provides a completely functional system ideal for evaluating the capabilities of the DS5250.

Getting Started with RSA Key-Pair Generation

The sample application binary (`rsa.hex`) and Sample Application code that generates the RSA key-pair can be obtained by writing to: micro.support@maxim-ic.com. See the section *Loading the Sample Application onto DS5250-KIT EV Kit* below for loading and running the sample application.

You build and execute the RSA key-pair sample application program written in C using the Keil μ Vision2 IDE.

1. Install the Keil μ Vision2 IDE.
2. Open the project `rsa.uv2`. The project file along with sample code can be obtained by writing to: micro.support@maxim-ic.com.
3. Click on **Project** \rightarrow **Rebuild All Target FILES** to generate the `rsa.hex` file.

Loading the Sample Application onto the DS5250-KIT EV Kit

The Microcontroller Tool Kit (MTK) is used to load the application onto the EV kit. The most recent version of the MTK application can be [downloaded from our site](#). To install MTK, run the installation file and follow the instructions. After a successful installation, a new menu group will be added: **Start** \rightarrow **All Programs** \rightarrow **Dallas Semiconductor MTK**. When MTK is launched, a dialog box similar to the one shown in **Figure 1** will be displayed.

If you encounter technical issues running MTK, your problem might be chronicled in the Maxim discussion board. You can search the existing posts and create new posts at: [Maxim Discussion Board](#).

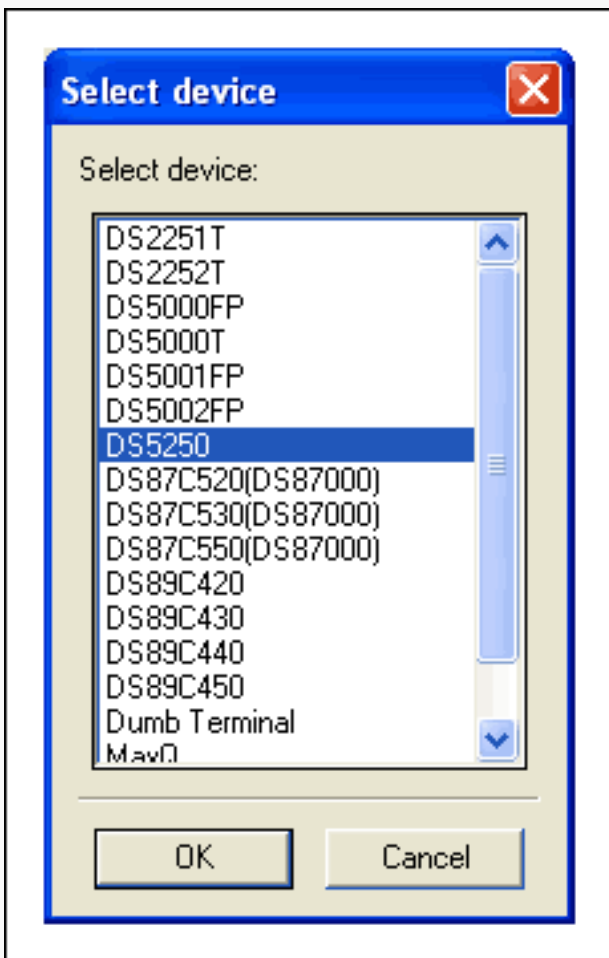


Figure 1. MTK options on startup.

Select the option **DS5250** to communicate to the EV kit. From the MTK menu, **Options** → **Configure Serial Port**, select the COM port which you are using and choose 115200 speed. Next select the **Target** → **Open COMx port at 115200 baud** option, and then **Target** → **Connect to Loader** to reset the EV kit. The DS5250 loader should print a message something like the following:

```
DS5250 SECURE LOADER VERSION 1.0 COPYRIGHT (C) 2002 DALLAS SEMICONDUCTOR
LID: 62E9490700000071 8284
```

>

Configure the EV kit memory by sending the following commands to the loader.

```
W MSIZE 121
W MCON 812
```

¹W MSIZE 12 identifies the external program and data memory chip size as 512Kb.

²W MCON 81 identifies the memory as Partition Mode.

From the **File** menu, select **Load HEX File** and then the `rsa.hex` file that you just created.

Choose **Target** → **Disconnect from Loader** to execute the program loaded onto the EV kit. The prompt appears as seen in **Figure 2**.

Enter key length bits to be generated:

Enter the number (for example, 1024) and wait for the application to display the results. The application displays the execution status as shown in Figure 2. It takes approximately 60 seconds to generate a 1024 bit-length RSA

key-pair, encrypt, and decrypt the random message. This time can vary for each execution. The minimum, maximum, and average times needed to generate an RSA key-pair for various bit lengths are tabulated in **Table 1**

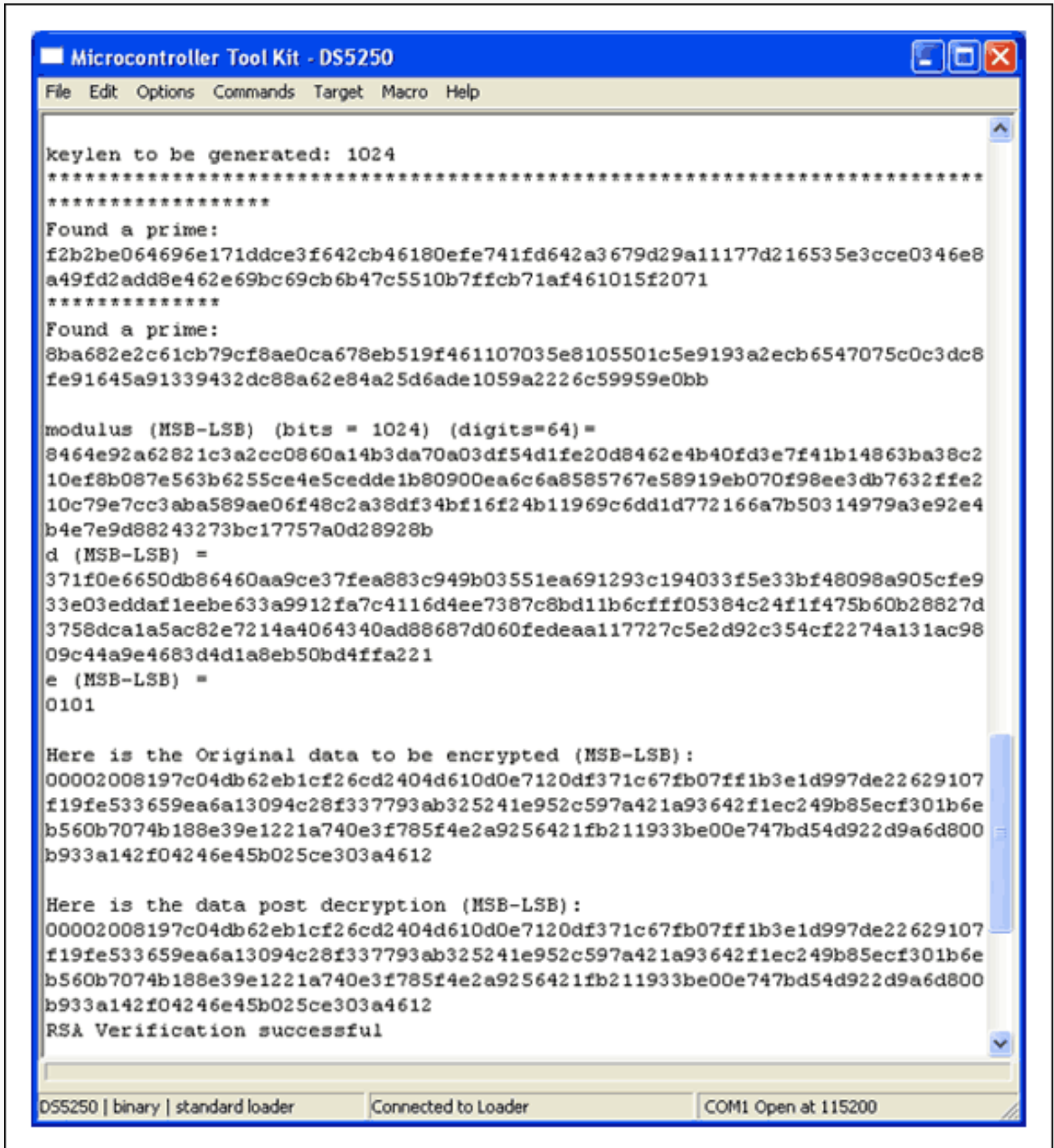


Figure 2. Execution status and results of sample application.

Developing a Simple Application Using RSA Key-Generation Library

The library provides four easy-to-use interface functions in C to generate the key-pair and encrypt/decrypt the user message using the private/public key. Refer to the `rsalib.h` file to see the prototypes of these interfaces. The application provided with this application note demonstrates the use of these interface functions:

```
rsa_generateKeySet(...)  
rsa_bignumModExp(...)  
rsa_newNum()  
rsa_freeNum()
```

Typical test results for different bit lengths are shown below.

Table 1. Average Time Needed for Generating an RSA Key-Pair

RSA Bit Length Generated	Number of Tests Run	Minimum Time Taken for the Test (in seconds)	Maximum Time Taken for the Test (in seconds)	Average Time Taken per Test (in seconds)
256	60	3.4	10.3	4.8
512	60	6.1	21.0	10.76
1024	60	13.5	62.0	26.6
2048	60	36.6	313.2	122.4
3072	30	102.7	731.9	369.8

Conclusion

The RSA key generation library provided by Maxim allows applications written in C to access the power and functionality of the DS5250 microcontroller hardware. RSA key-pairs can be generated up to a maximum of 4095 bits.

Relevant Links

Application note 2783, "[Using the Keil C Compiler for the DS5240/DS5250](#)"
[Secure Microcontroller Family User's Guide and Supplements](#)
[DS5250 High-Speed Secure Microcontroller Data Sheet](#)

µVision2 is a registered trademark of Keil Corporation.

Application note 4004: www.maxim-ic.com/an4004

More Information

For technical support: www.maxim-ic.com/support
For samples: www.maxim-ic.com/samples
Other questions and comments: www.maxim-ic.com/contact

Automatic Updates

Would you like to be automatically notified when new application notes are published in your areas of interest?
[Sign up for EE-Mail™.](#)

Related Parts

DS5250: [QuickView](#) -- [Abridged Data Sheet](#)

DS5250: [QuickView](#) -- [Abridged Data Sheet](#)

AN4004, AN 4004, APP4004, Appnote4004, Appnote 4004

Copyright © by Maxim Integrated Products

Additional legal notices: www.maxim-ic.com/legal