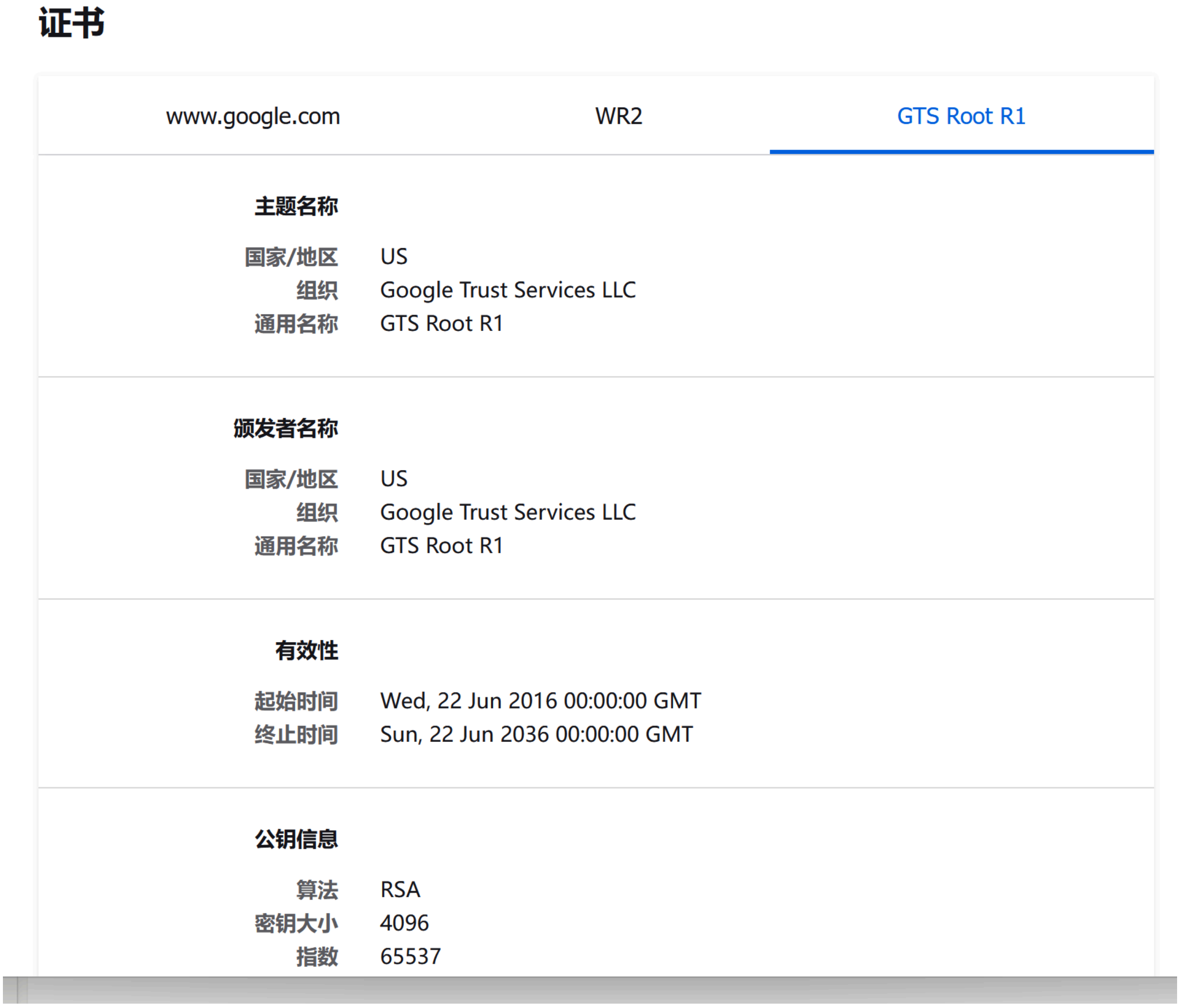
COMP7906 Introduction to Cyber Security

Assignment 3

ZHANG Hongyi

Q1

PKC Screenshot



证书

主题名称

国家/地区	US
组织	Google Trust Services LLC
通用名称	GTS Root R1

颁发者名称

国家/地区	US
组织	Google Trust Services LLC
通用名称	GTS Root R1

有效性

起始时间	Wed, 22 Jun 2016 00:00:00 GMT
终止时间	Sun, 22 Jun 2036 00:00:00 GMT

公钥信息

算法	RSA
密钥大小	4096
指数	65537

The screenshot of the PKC of www.google.com in Firefox is shown above.

Issuer (CA)

The issuer of the PKC is **Google Trust Services** according to the detailed information.

Signing algorithm and the key length

In Firefox, the signing algorithm is shown as **RSA**. And the key length of it is **4096 bits**.

Q2

Alice's private key

$$\begin{aligned} n_A &= 77 \\ &= 7 \times 11 \end{aligned}$$

$$p = 7, q = 11$$

Since $e_A = 23$, and $e_A \times d_A \equiv 1 \bmod \varphi(n)$, $d_A = \frac{k\varphi(n)+1}{e_A} = \frac{60k+1}{23}$, $k \in \mathbb{N}$.

Thus, we can calculate the value of d_A:

$$d_A = 47$$

So, Alice's private key $(d_A, n_A) = (47, 77)$.

The value of the plaintext m

According to RSA, $m = c^{d_B} \bmod 91 = 82$.

So the plaintext m is **82**.