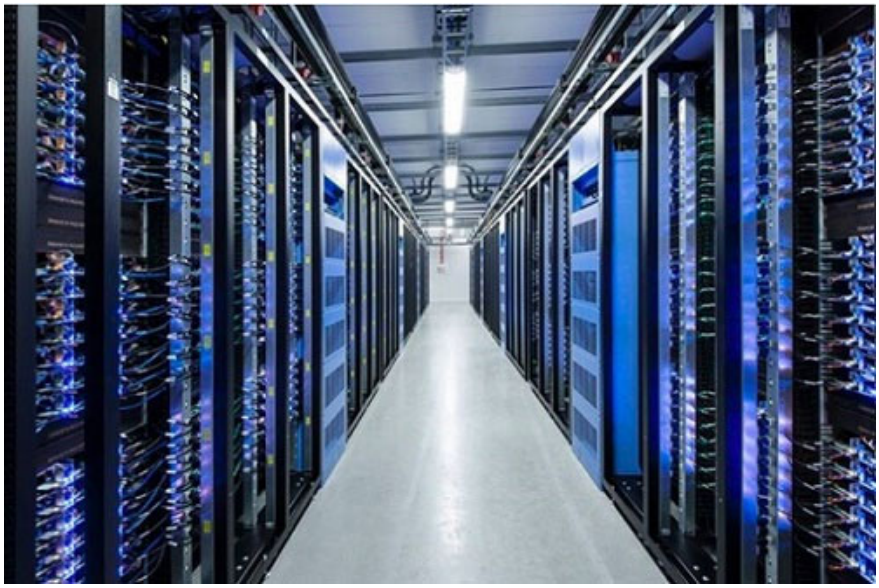
Google raises data security with 2048 bit encryption

In a message released on Monday, Google said it would transfer all certificates to use 2048 bit encryption. The certificates are used to encrypt the communication between the server and the user's web browser.

To access Google's transmission data, hackers or NSA will have to cross the 2048 bit encryption wall.



In a message released on Monday, Google said it would transfer all certificates to use 2048 bit encryption. The **certificates** are used to encrypt the communication between the server and the user's web browser.

This has great implications: hackers and NSA can hardly pass the encryption, because Google no longer uses the old 1024-bit encryption standard. This step can be considered a response to the NSA, with 2048 bit encryption, tracking user information, whether legal or not, will become much more difficult. According to Google, the company has passed its internal term to implement this step. Google and Yahoo are also currently performing data encryption between their internal data centers.

In the future, Google will also switch to supporting " *forward secrecy* " standard. Accordingly each server session will have its own encryption key. The encryption key for each sent message will not be able to decrypt previous messages.