**Activity 12-1: Creating a Substitution Cipher**

**Step 1: Plaintext Message**

Our group wrote a five-word message about the teacher.

**Plaintext:  
Professor Polyakov is an excellent teacher**

**Step 2: Substitution Cipher Used**

Next, we created a simple substitution cipher using a Caesar shift of +3. This means every letter in the message is moved three letters forward in the alphabet.

**Examples:**

A → D

B → E

C → F

D → G

E → H

F → I

G → J

H → K

I → L

J → M

K → N

L → O

M → P

N → Q

O → R

P → S

Q → T

R → U

S → V

T → W

U → X

V → Y

W → Z

X → A

Y → B

Z → C

Spaces between words stay the same.

**Step 3: Ciphertext (Encrypted Message)**

After applying the +3 shift to each letter, we encrypted the message.

**Ciphertext:  
Surihvvru Srobdnry lv dq hafhoohqw whdfkhu**

**Step 4: Sharing the Ciphertext**

When the instructor asked us to, we shared our encrypted message with the other groups so they could try to decrypt it.

**Step 5: Decryption**

The other groups decrypted the message by shifting each letter back by 3. When a group finished decrypting it correctly, the group leader said “Finished!”

**Step 6: Discussion**

After all groups finished, we discussed:

* The type of substitution cipher used
* How easy a Caesar cipher is to break
* Why stronger encryption is needed in real-world security

**Activity 12-2: Securing Personal Communication Using Encryption**

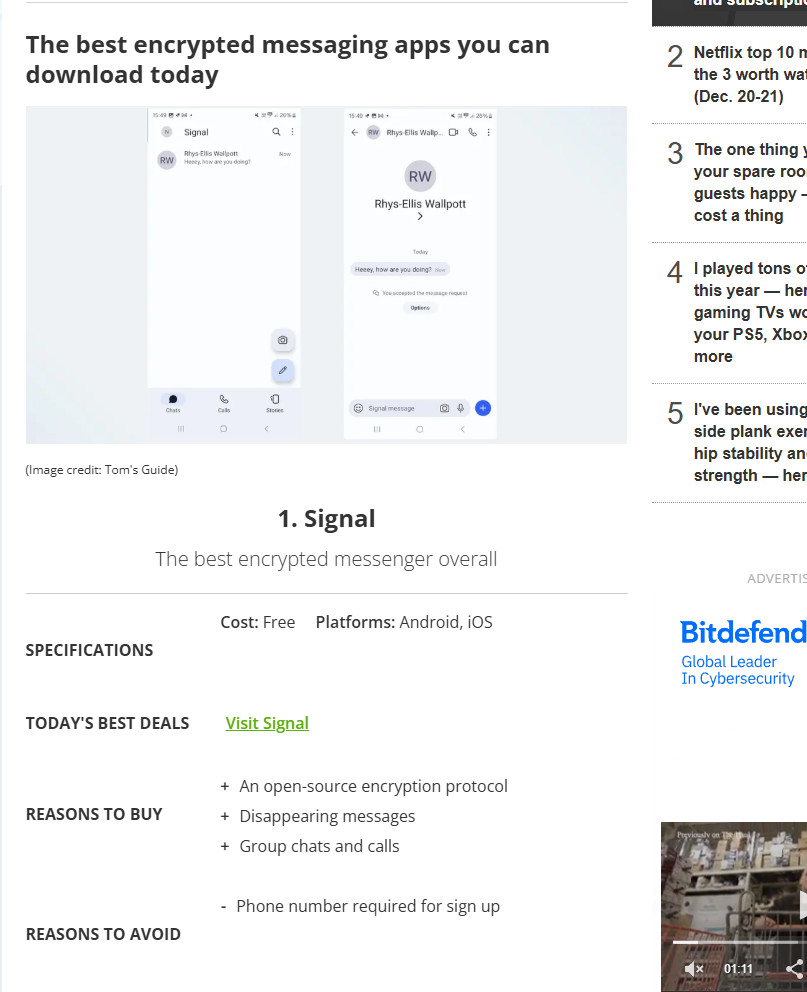
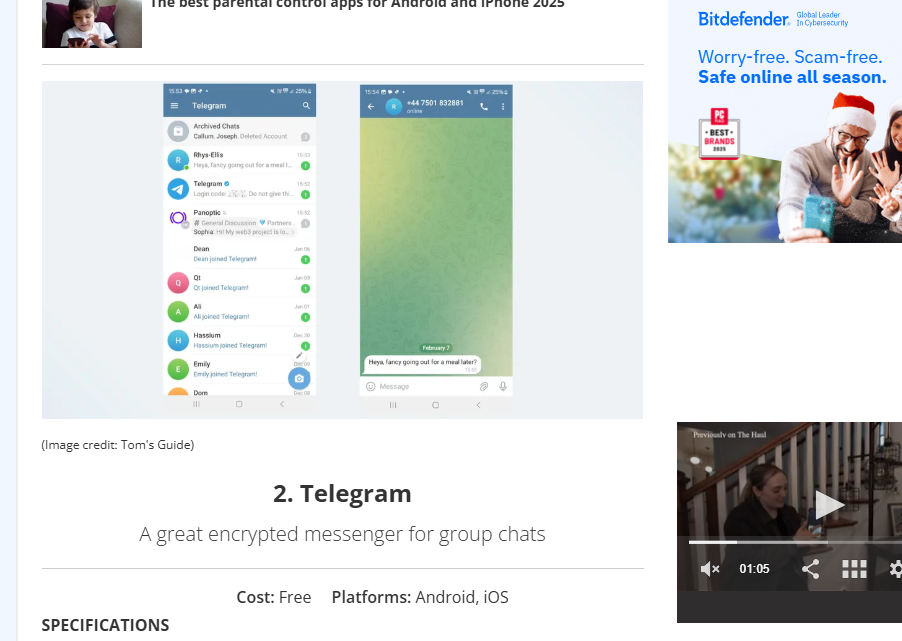
**Step 1: Open a web browser**

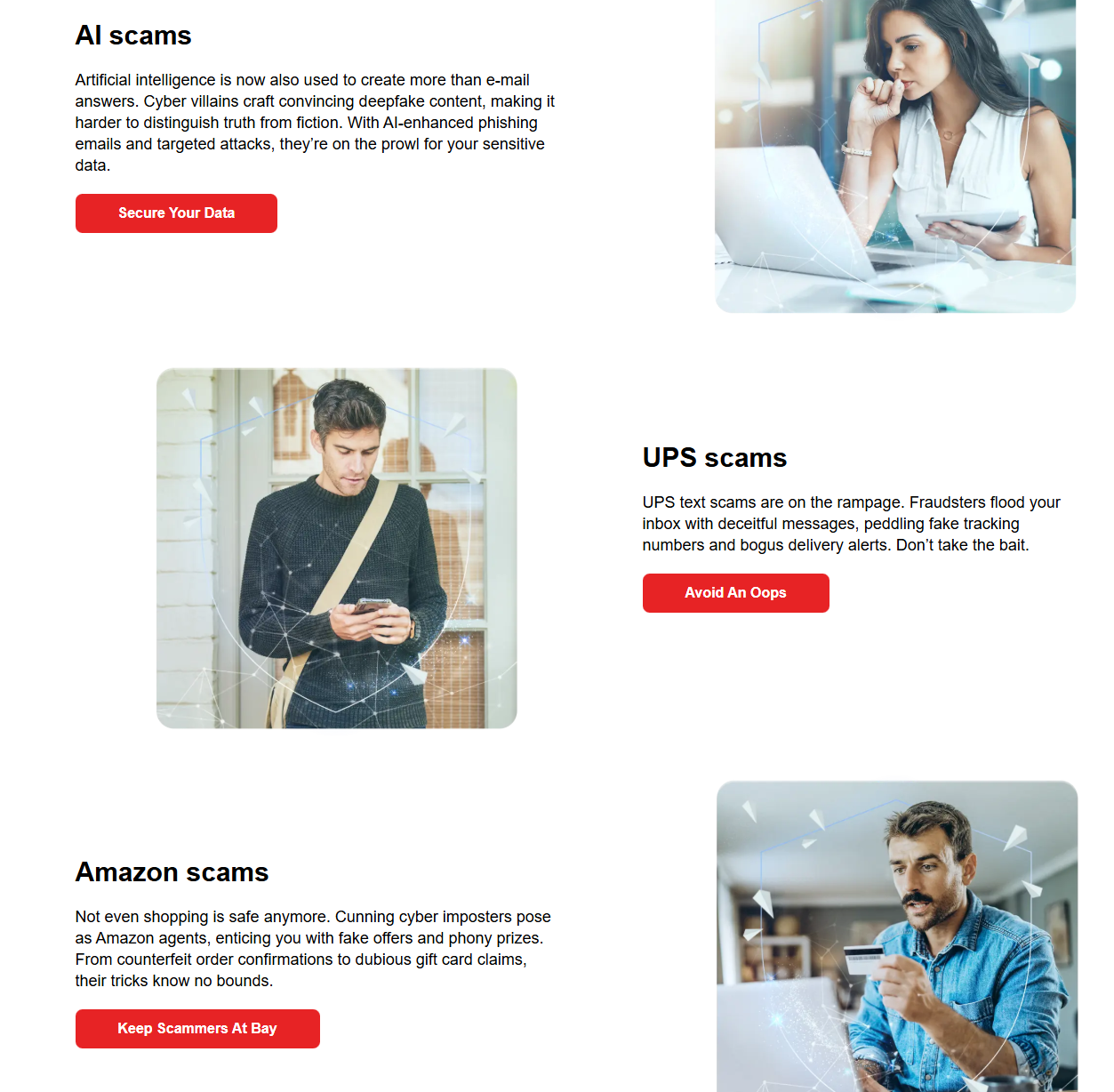
First, I opened a web Google Chrome on Windows



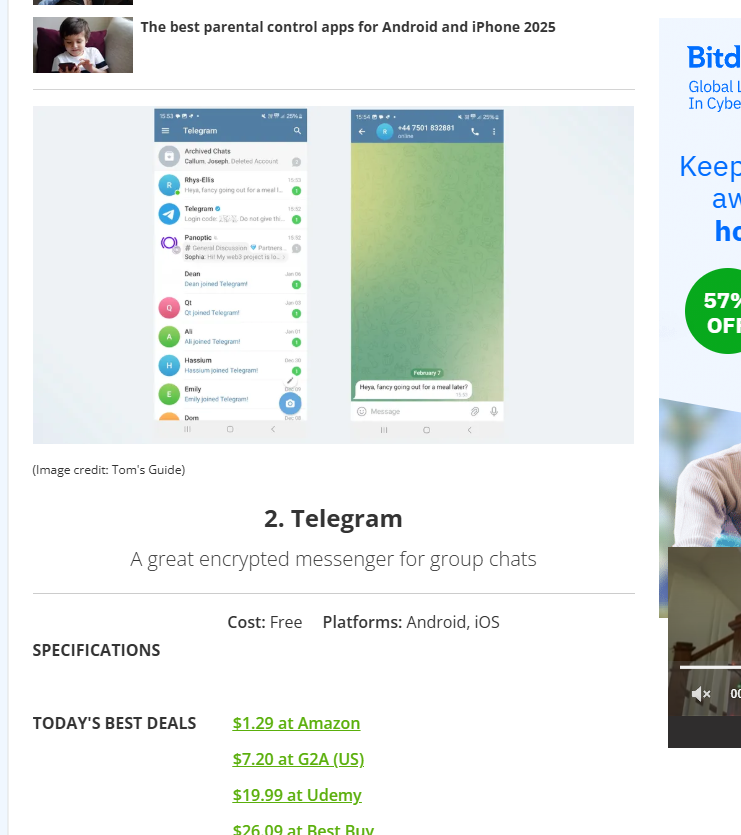
Step 2: Reading the article and answering the questions

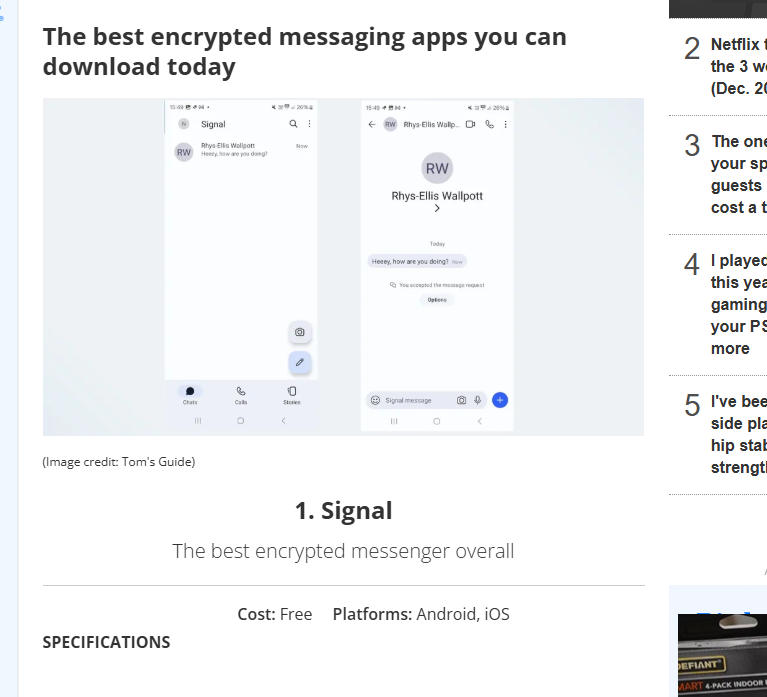
I read the Tom’s Guide article about the best encrypted messaging apps. From the article, I learned that there are many apps available that help protect personal communication using end-to-end encryption.

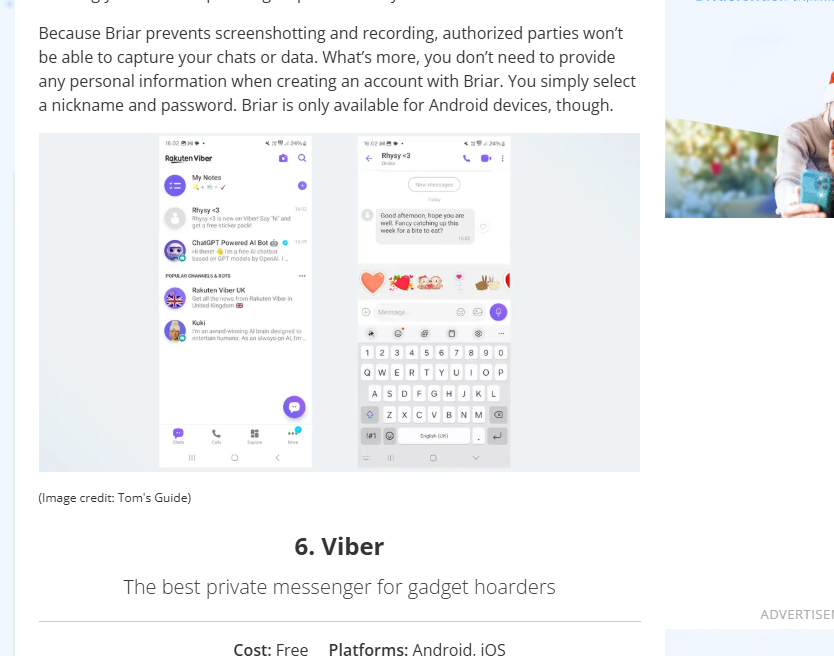




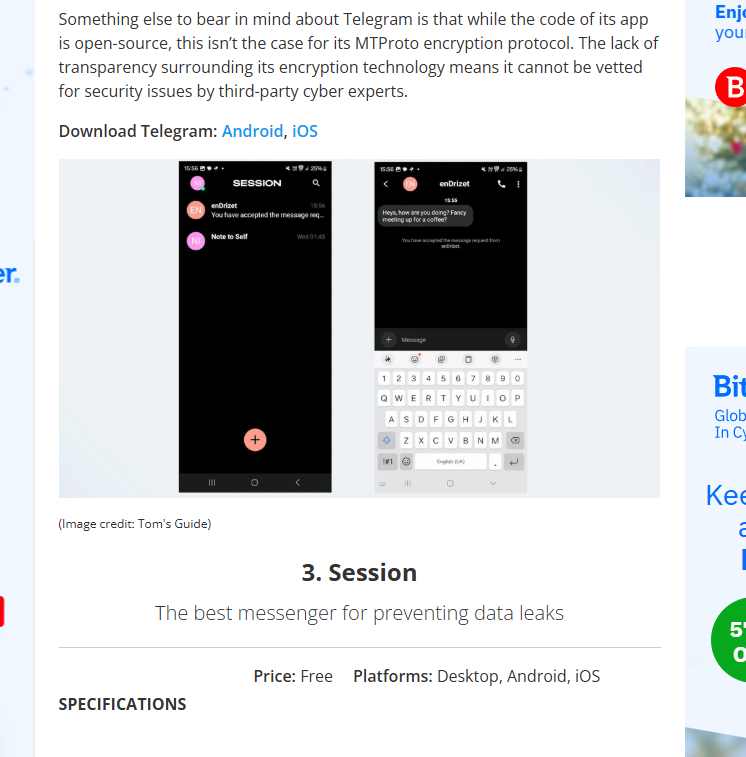
Some of the main apps mentioned in the article are Signal, Telegram, Session, WhatsApp, Briar, and Viber. These apps use encryption so that only the sender and the receiver can read the messages.

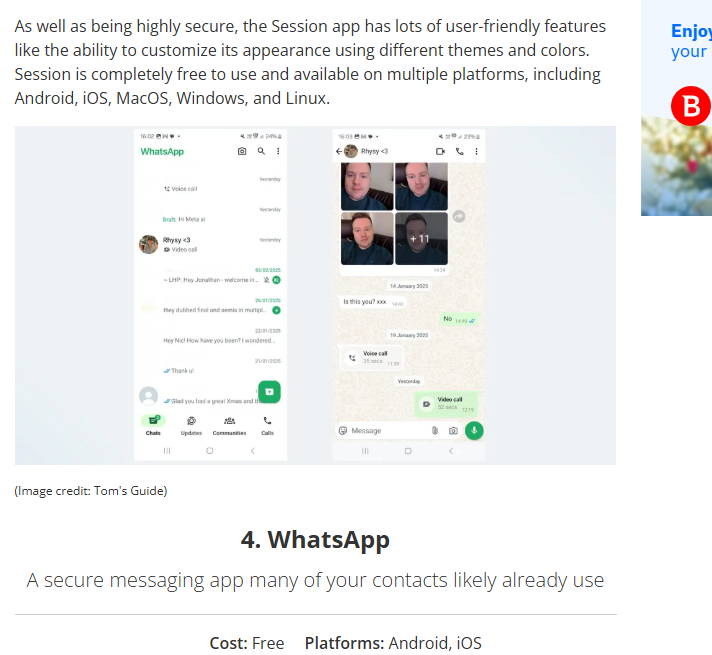






I currently use WhatsApp, and I already knew that it uses encryption, but I did not know that it uses the Signal Protocol and that all messages, calls, and media are encrypted by default. Reading the article helped me understand this better.



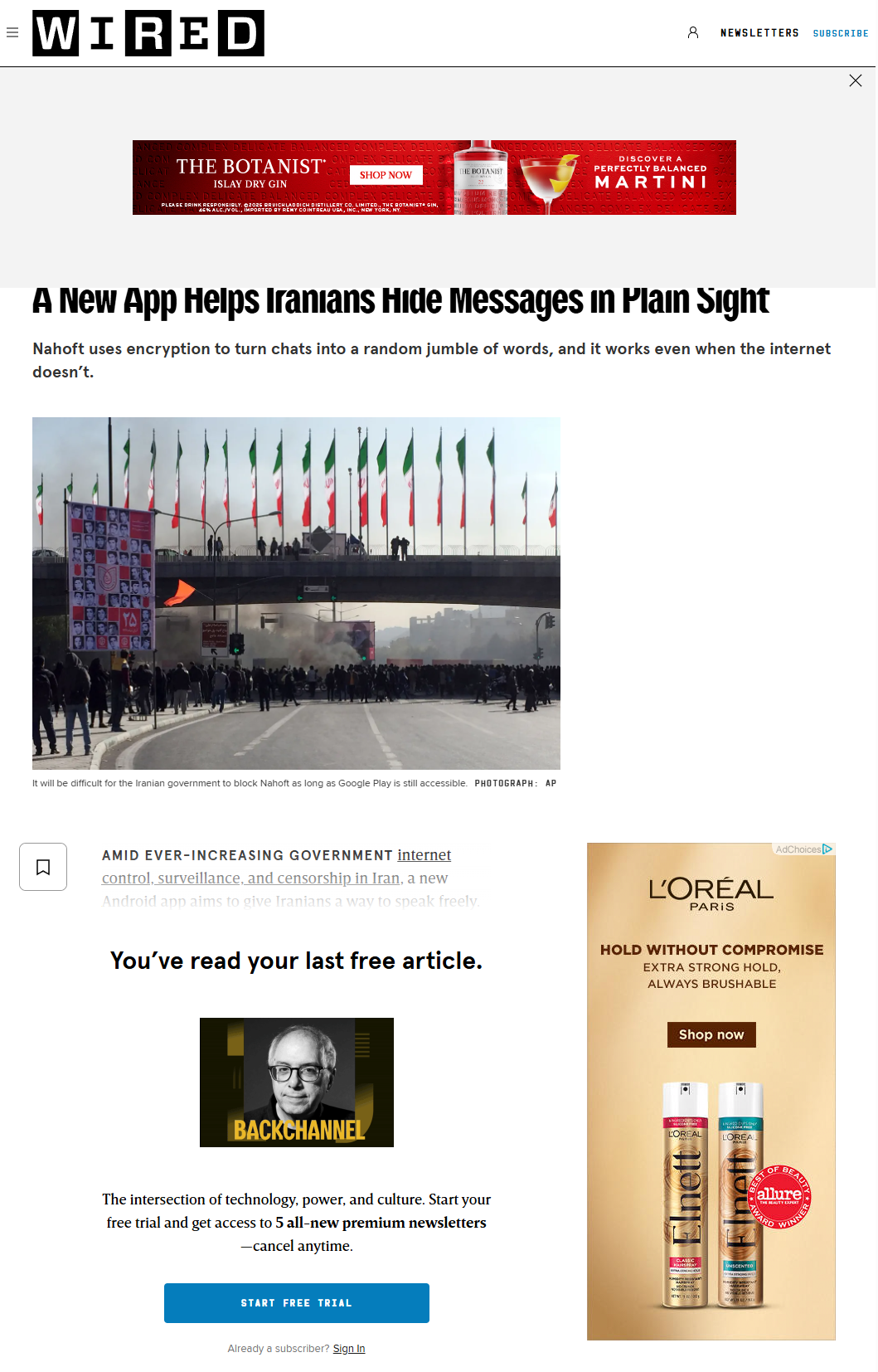


I was also aware that some apps, like Facebook Messenger, have encryption options, but I learned that encryption is not enabled by default and users have to turn on features like secret conversations to get encrypted messaging.

This article helped me understand, this article/plugin helped me understand the different encrypted messaging options available and why it is important to use encrypted apps to protect personal communication and privacy.

**Step 3: Reading the Wired article**

I used my web browser to open and read the article on **Wired** at  
[**www.wired.com/story/nahoft-iran-messaging-encryption-app/**](http://www.wired.com/story/nahoft-iran-messaging-encryption-app/).





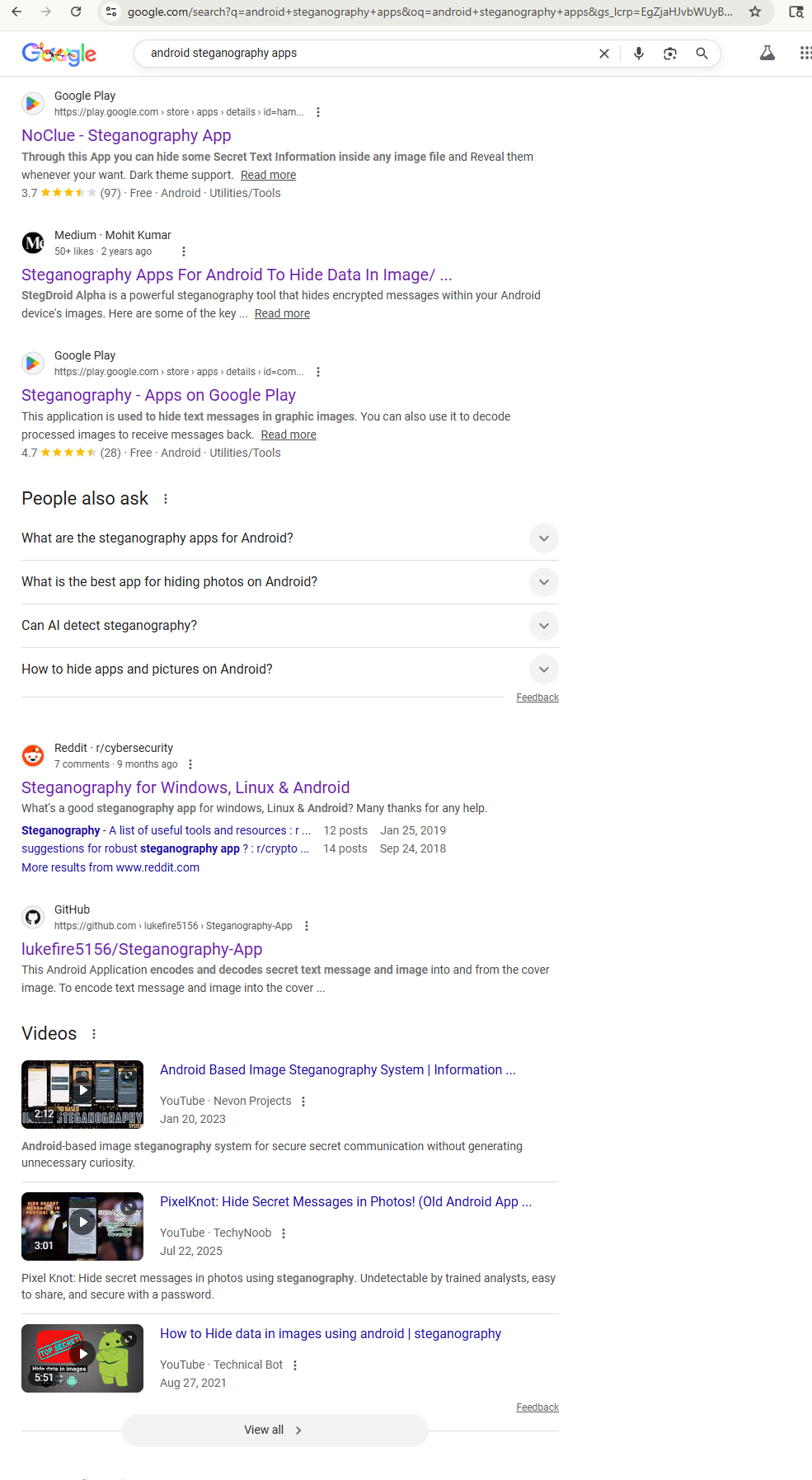
The article explains how the Nahoft app helps people hide messages using encryption in places where communication is monitored.

**Step 4: What basic type of cryptography does the Nahoft application use?**

The Nahoft app uses steganography with encryption. Instead of just encrypting the message, it hides the encrypted text inside ordinary-looking words so it doesn’t look like a secret message. That way, even if someone sees the message, they won’t know it contains encrypted information unless they know how to extract and decrypt it.

**Step 5: Searching for Android steganography apps**

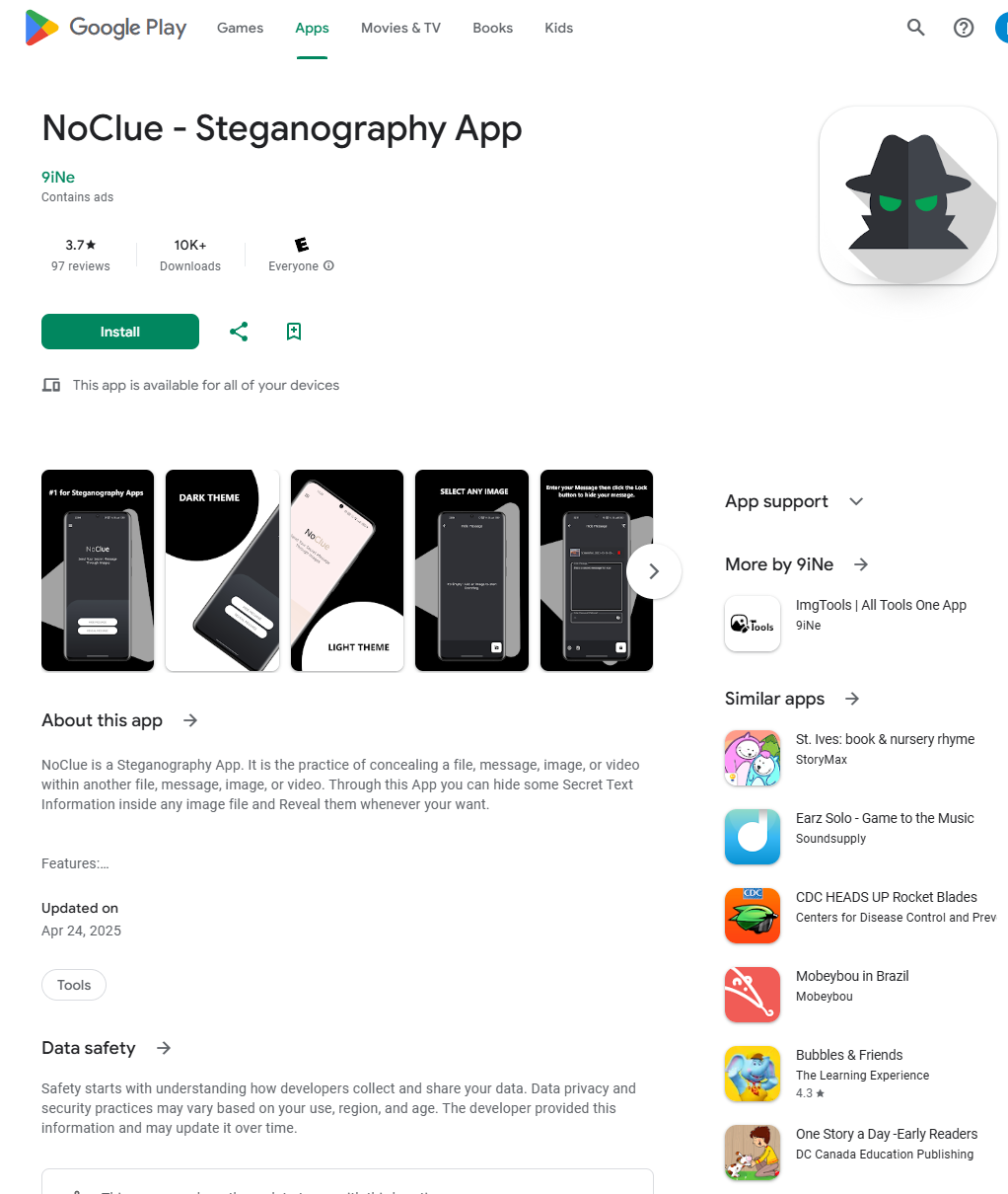
I used my web browser and searched for **android steganography apps.** From the search results, I found several apps and articles related to hiding messages inside images and files on Android devices.

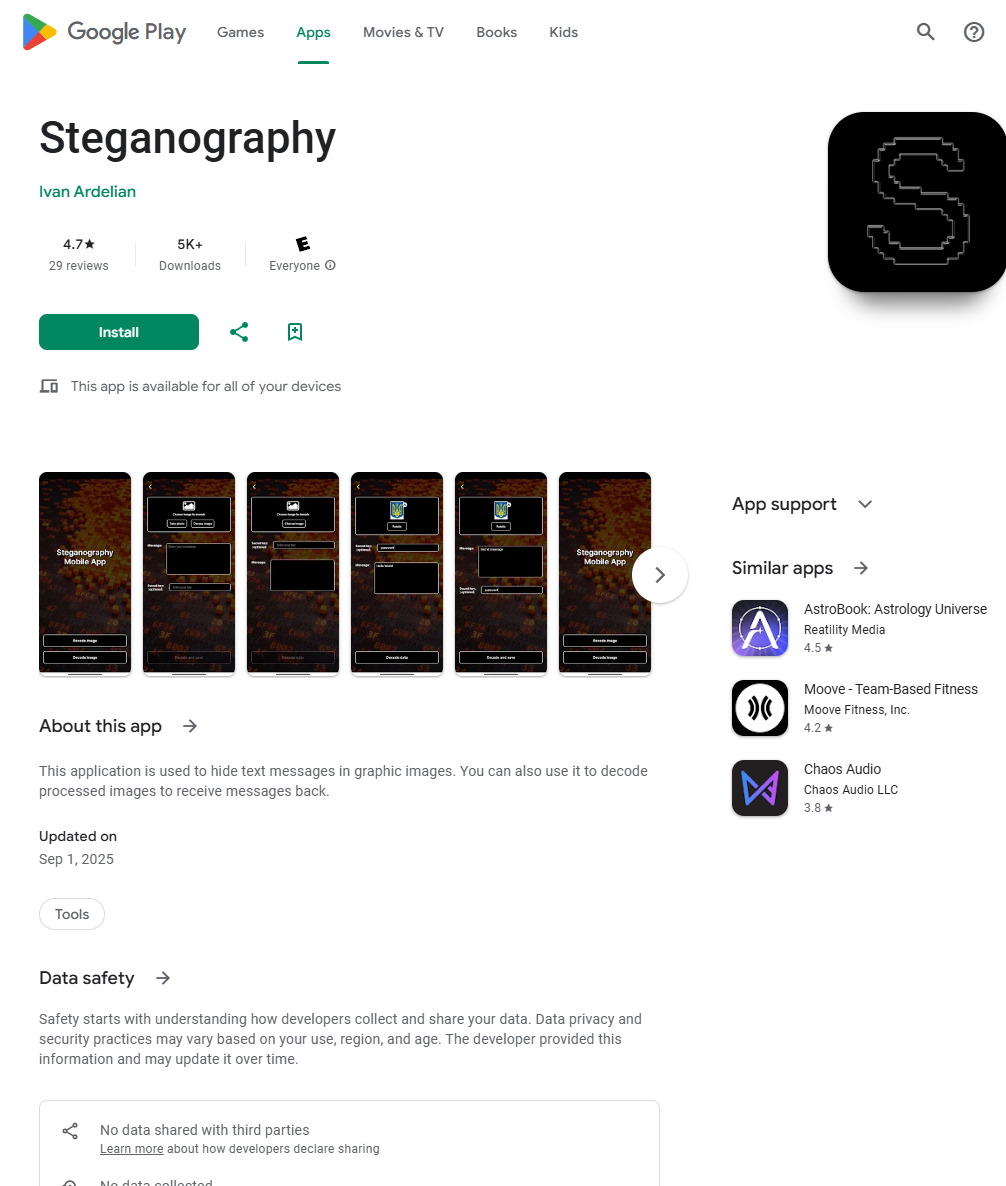


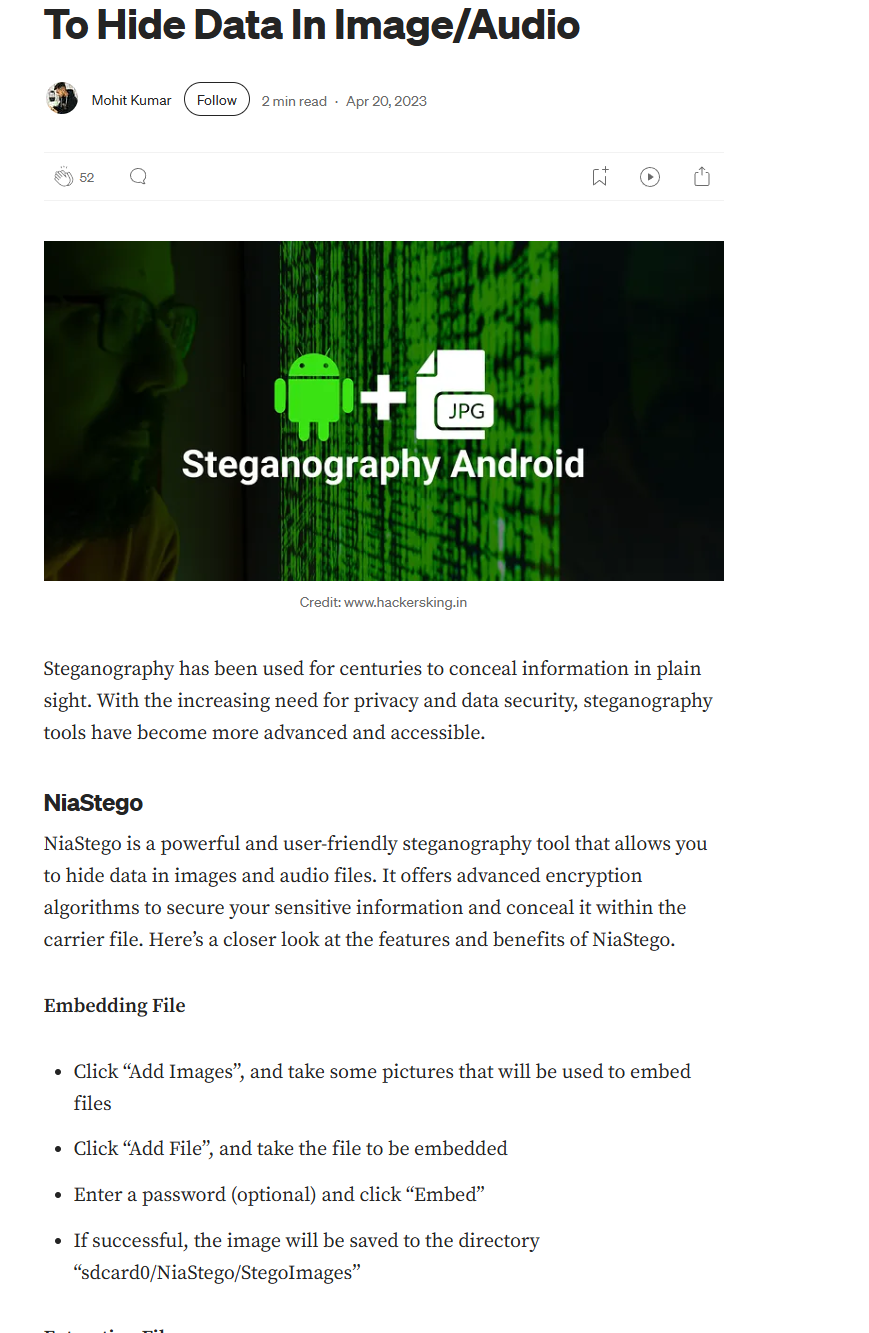
**Step 6: Steganography explanation and examples**

**What is steganography?**

Steganography is a technique used to **hide secret information inside another file**, such as an image, audio file, or video, so the message is hidden in plain sight and does not look suspicious.







**Examples of Android apps that use steganography:**

* **NoClue – Steganography App** (hides secret text inside images)
* **Steganography App (by Ivan Ardelian)**
* **NiaStego** (hides data in image or audio files)

I tried one of these apps with a friend by hiding a short message inside an image and then sharing the image. The message could only be read after decoding it using the same app.

**Step 7: Exit**

After completing the activity, I closed the web browser and logged off Windows to prepare for the next activity.

**Activity 12-3: Creating a Rogue Server Certificate by Breaking a Hashing Algorithm**

**Step 1:**

I started a web browser in Windows and went to [**www.google.com**](http://www.google.com)

**Step 2:**

I typed creating a rogue ca certificate into the search bar and pressed Enter. I clicked the first link in the search results, which opened the Rogue CA research page on Phreedom.org.



**Step 3:**

**How many of the 30,000 certificates were signed with MD5?**

Out of 30,000 website certificates collected in 2008, 9,000 certificates were signed using MD5.

**What kind of hardware was used to generate the chosen-prefix collision?**

**How much money was spent on certificates?**

The researchers used a cluster of 200 PlayStation 3 consoles to generate the chosen-prefix collision. They spent a total of USD $657 on certificates.

**What was the impact of generating a rogue CA certificate?**

**What would this allow a malicious attacker to do?**

Generating a rogue CA certificate allowed attackers to issue fully trusted SSL certificates. This would enable undetectable man-in-the-middle attacks, phishing, and impersonation of secure websites such as banking and e-commerce sites.

**Which hashing algorithm were CAs forced to use after MD5 was shown to be insecure?**  
After MD5 was demonstrated to be insecure, Certificate Authorities were forced to switch to SHA-1.

**According to the researchers, what is the only way to effect change and secure the Internet?**  
According to the researchers, **making theoretical attacks practical** is the only way to effect change and secure the Internet.

**Step 4:** I closed all open windows.