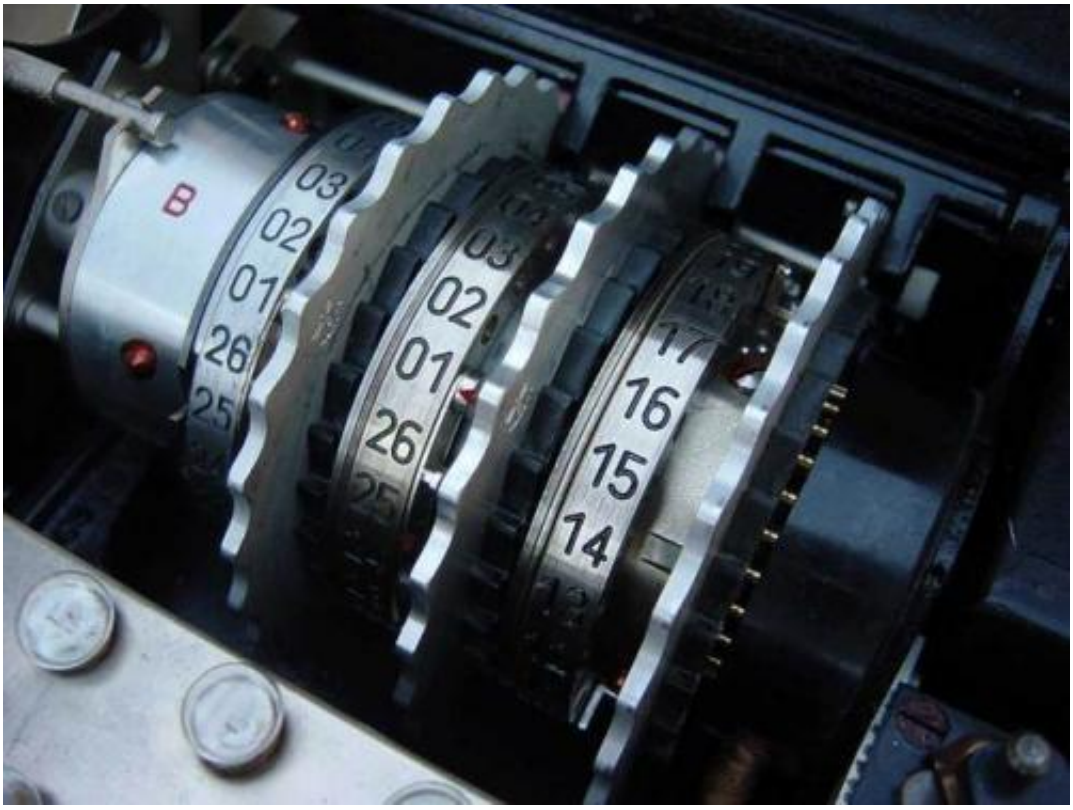
It's all about cryptography as Rusbridger faces parliament

December 5 2013, by Eerke Boiten



The big questions in the Snowden saga hinge on who knows what about encryption. Credit: Bob Lord

Despite all the political blustering that has surrounded Guardian editor Alan Rusbridger's meeting with the House of Commons Home Affairs Committee this week, the real story in the Snowden affair is cryptography.

In some ways, it seemed as though UK security agency GCHQ had been hit by the notorious CryptoLocker virus. CryptoLocker holds computer users to ransom by encrypting all their files and can cause serious headaches for the victim. Some of the answers given by Guardian editor Alan Rusbridger at the House of Commons Home Affairs Committee on 3 December paint a picture similar to what happens when the virus strikes.

Rusbridger admitted that David Miranda, the partner of Guardian US columnist Glenn Greenwald, had been carrying some of the Snowden files in encrypted form when he was held under the Terrorism Act in August. But, so far, neither the police nor GCHQ have been able to decrypt them.

So, just like CryptoLocker victims, GCHQ is in possession of some of its own files but cannot get into them, as much as it would like to. The contents of the files won't be a surprise, but GCHQ would very much like to know what it is that Snowden and the journalists know about its work.

Encryption lay at the heart of some of the most important exchanges during Rusbridger's hour-long appearance in front of MPs. There were some odd interventions at the start of the session, including committee chairman Keith Vaz's questioning of Rusbridger over whether or not he loved Britain, but from then on, one issue dominated proceedings. This was the transfer of a copy of the Snowden files by the Guardian to the *New York Times*.

Rusbridger made it clear that the Guardian had indeed shared its entire collection of Snowden files with its American partner. This had been done for journalistic collaboration, and as a safeguard after the pressure put on the Guardian by the UK government over the project.

These files had not been redacted to remove the names of intelligence staff but had largely been transferred in a way that Rusbridger considered fully secure. He reiterated both these points repeatedly in response to near-identical questions from the Committee. Some of the MPs argued that the Guardian might have committed an offence by transporting secret materials to a foreign country, especially if it had not encrypted them securely.

A cryptographic contradiction

A contradiction remains after Rusbridger's evidence session relating to cryptography, and it's one that is crucial when we think about whether or not The Guardian overstepped the mark in the Snowden affair.

When pressed for details of the security arrangements for the Guardian's Snowden files, Rusbridger was reluctant to provide an on-the-spot answer and offered to provide written details to the committee later.

This seemed somewhat unusual. It is well accepted in information security circles that it is undesirable to provide "security through obscurity". This is where your security depends on outsiders not knowing what methods you used – rather than proving security by revealing known strong methods.

Faced with an audience of security specialists, Rusbridger might have inspired some confidence by stating, say, that they used AES with 256-bit keys. But that kind of tech-talk doesn't play well with a parliamentary committee, which isn't equipped with the specialist knowledge required to appreciate it. Thus, all he said on this was that the files were protected with "military-grade" encryption, and that his newspaper had fully acknowledged and acted upon the unique level of sensitivity of these documents.

However, The MPs' questions appeared at times to be based on the assumption that the transfer and storage of the Snowden documents had indeed been insecure. A Cabinet Office spokesman was also reported as stating after the meeting that "The Guardian's publication and non-secure storage of secret documents has had a damaging effect on our national security capabilities.".

This "fact" of non-secure storage was not established in the House of Commons meeting, and in any case the committee did not appear to have the competence to make such a judgement. So why is it still assumed?

Very speculatively, it may be that the data seized from David Miranda have revealed more to GCHQ about the security arrangements taken by the Guardian than Rusbridger thinks. If this is the case, perhaps Rusbridger has overestimated the ability of the security arrangements used to protect the data. This may even undermine the confidence previously expressed in encryption by Snowden, Greenwald and security experts.

If that were the case, it raises interesting questions about whether good faith in the encryption you are using is a sufficient defence. If your adversary is the NSA or GCHQ, the Snowden files themselves already tell you they have ways of circumventing it …

The real questions that need to be asked

In its ongoing inquiry into this affair, the Home Affairs Committee will take evidence from MI5 chief Andrew Parker next week. Although there is no suggestion that he will be fully briefed on the questions in advance this time, there are some questions that he can probably guess. Top of the list must be: how could Snowden get access to so many highly sensitive files?

This question has been raised several times by Liberal Democrat committee member Julian Huppert – and indeed by Rusbridger in this inquiry. The Guardian and its editor aren't the only ones that need to provide a clear picture of their understanding of security and cryptography when explaining their role in this affair.

Provided by The Conversation