7/27/16 - Final Exam - Erik Buschardt

Q2: Discuss the debate between **privacy/individual freedoms vs. security and law enforcement** in regards to managing public key and encryption techniques. Include in your discussion both ethical and legal issues. Finally, include in your answer your view of the topic and support it with logic and reason.

With regards to the Edward Snowden debate at NYU against Fareed Zakaria of CNN, my position is clear. The mathematics of encryption are non negotiable and uncompromisable. There is no way to maintain security of a back door or any side door to the process of encryption without a significant corruption of policy in the long term. I believe that Mr. Snowden was right on the money when he stated (and I paraphrase) that a court is nought but a humble human construct, subject to the legitimacy of the government for which it was built to uphold. This means that at the end of the day, the court is only as legitimate as the government itself, which is saying a lot when speaking of certain corrupt governments that happen to stand partially or totally against us on cherished democratic issues (such as Iran, Russia, China and North Korea to name but four).

Ethical issues will include the moral dilemma (think "1984") of government snooping on innocent persons with greater ease than ever before, while maintaining a threat of conviction over our heads, and "lowering the bar" or burden of proof if you will, by introducing to our court system only a relatively quick-minded suspicion, in order to obtain evidentiary proof of conviction, rather than having actual thought-out and harder-to-obtain reasoning for a warrant for search and seizure. To a lesser extent, the Fourth Amendment will play a greater role in that which is to be searched, rather than seized until <u>after</u> any arrests or raids, because of the nature of modern technology (not to mention the data mining capabilities of social media post 2004), and the power of pilotless drones, zoom-cameras, heat sensors, infrared, night vision, and all other manners of modernized search.

Back to the topic at hand of encryption and cryptology, we see that policy-driven back doors are inherently a bad idea. The burdens of a legal prosecution in order to build a case <u>absolutely</u> <u>should</u> <u>not</u> be lowered to the extent that said burdens to obtain meaningful evidence are now trivial, as in the case of the San Bernardino iPhone, according to Mr. Snowden's effective argumentation.

Q3: Provide an overview of the purpose of the **One Way Hash** functions, how they work, the application of their use, and the issues (advantages and disadvantages) of hash functions to encryption methods.

One Way Hash functions digest or compile a message, turn such a digestion into a string of data into what is called a hash, associated with a key, in order to produce a robust transmission that is both integral because of the hash, and authentic because of the key. Because of this fact, they are deemed irrefutable to the sender, due to the mathematical certainty placed in the algorithmic process. An obvious disadvantage is that the hash is not able to be reverse-engineered, so as to be re-used. This means that for better or for worse, the hash is unique to the message itself, and that a new key must be generated for each transmission.

Q4: Outline the definition, uses, importance, and issues with **Diffusion and Confusion**, and explain why these properties are important to the the design of robust hash functions and pseudorandom number generators.

Confusion is a substitution function whereby plaintext letters are swapped out for ciphertext letters, (IBM → HAL for example). Diffusion is a transposition function where plaintext letters (in ASCII format but nowadays including UNICODE) are mixed throughout the message in order to create an encrypted, or mixed up, message. Both methodologies are integral to the successful implementation of hash functions (by maintaining traces of the message itself without development of a key from which to reverse-engineer the transmission) and pseudorandom number generators, (by generating a ciphertext in such a manner as to produce as unique a value as is computationally possible).

Q5: Discuss **Data Encryption Standard (DES)** to include its genesis, the public/private partnership from its beginnings, the groundbreaking impact it has had on modern encryption, how it works, issues (advantages and disadvantages) and your overall assessment of DES and what it meant to the science of encryption.

To summarize, when the precursor to the NIST put out a public request for an encryption policy, strategy and effective algorithm, many applied but few designs qualified. When a second request was subsequently published, a team from IBM had already developed an effective algorithm strategy but was reluctant to publish it. In the end, a confusion and mistrust developed between the developers at IBM and the NIST authority, where the details of DES were not disclosed but rather kept secret, as was not the intent.

DES works via a combination of substitutions and transpositions applied with an asymmetric key. As we witnessed via YouTube with a 56-bit example, the bits were scrambled a series of times before being transpositioned exactly once before and once after the substitution process involving the key. As we can imagine, there are infinitely many ways one can mix and match bytes in order to maintain a reasonable threshold of integrity of the message, and DES was one of the more effective and elegant methodologies applied in recent memory. That would be one advantage of DES (its elegance and straightforward application), while its obvious disadvantages is that since then, it has been broken and therefore rendered obsolete.

My impressions of DES are very favorable in that it was and remains the gold standard of all modern encryption implementation strategies. Its processes of transposition and substitution provide a recipe for a successful integrity and irrefutability of any transmission. Its efforts need only be duplicated (in the case of 3DES) in order to provide even more security to the end user, proving that DES was indeed groundbreaking technology.