Supplemental Reading for The Future of Cryptanalysis

**It’s been said that the advent of modern computing has spelled the death of the field of cryptanalysis; but the practice is still alive and well -- it’s the methodology that’s changed as technology has transformed the landscape. As quantum computing continues to develop, there’re concerns that modern encryption could be at risk of being broken. This is because most modern encryption algorithms are based on large prime** [**number factorization**](https://en.wikipedia.org/wiki/Integer_factorization) **being computationally difficult, something that can be significantly sped up by quantum computing. Because of this, quantum computing would allow for significantly faster factorization and brute-force attacks on encryption keys, making the future of modern cryptography questionable in the looming quantum computing era.**

# Supplemental Reading for Symmetric Encryptions

## For more information about symmetric encryptions, check out the following link [here](http://www.rc4nomore.com/).

# Supplemental Reading for Asymmetric Encryption Attack

### An asymmetric encryption attack happened in 2010 to [Sony with their Playstation 3](https://nakedsecurity.sophos.com/2012/10/25/sony-ps3-hacked-for-good-master-keys-revealed/) game console. It turns out they weren’t ensuring the randomized seed value was changed for every signature. This resulted in a hacker group called 'fail0verflow' being able to recover the private key that Sony used to sign software for the platform. This allowed modders to write and sign custom software that was allowed to run on the otherwise very locked down console platform. This [resulted in game piracy](https://www.theguardian.com/technology/gamesblog/2011/jan/07/playstation-3-hack-ps3) becoming a problem for Sony, as this facilitated the illicit copying and distribution of games, causing a significant loss in sales.

# Supplemental Reading for SHA1 Attacks

## During the 2000s, a bunch of [theoretical attacks](https://eprint.iacr.org/2005/010) against SHA1 were [formulated](https://www.schneier.com/blog/archives/2005/02/sha1_broken.html) and some [partial collisions](https://eprint.iacr.org/2007/474) were demonstrated. In early 2017, the first [full collision of SHA1](https://shattered.io/) was published.

# Supplemental Reading for the X.509 Standard

## For more information about this topic from this Video Lecture check out the following link. The [X.509 standard](https://www.ietf.org/rfc/rfc5280.txt) is what defines the format of digital certificates.

# Supplemental Reading for PGP

## PGP was [developed by Phil Zimmermann in 1991](http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html) and was freely available for anyone to use.

# Supplemental Reading for Securing Network Traffic

## The combination of L2TP and IPsec is referred to as L2TP/IPsec and was officially standardized in [IETF RFC 3193](https://tools.ietf.org/html/rfc3193).

## An example of this is [OpenVPN](https://openvpn.net/index.php/open-source.html), which uses the OpenSSL library to handle key exchange and encryption of data along with control channels.

# Supplemental Reading for TPM Attacks

## There’s been one report of a [physical attack on a TPM](https://gcn.com/Articles/2010/02/02/Black-Hat-chip-crack-020210.aspx) which allowed a security researcher to view and access the entire contents of a TPM.