**Cryptography, Part 1, 9/4/2018**

* Encryption is term that is commonly used in our media, but few people understand what it is.
* Whether we realize it or not, we use encryption all the time when we log into a computer, browse the web using SSL, or use an iOS (and some Android[[1]](#footnote-1)) devices, which have full-disk encryption turned on by default.
* Cryptography is foundational to information security. It provides:
  + Confidentiality (or secrecy)
  + Integrity—ensuring that the contents of a message have not been tampered with.
  + Authenticity—proving who a message came from, or who performed a transaction.
  + Non-repudiation—ensuring that a party can’t back out of a transaction by claiming that they didn’t participate in a transaction.
* Cryptography is ancient—first recorded use was Egyptian hieroglyphics.
  + <http://www.cypher.com.au/crypto_history.htm>
* Historically, technological advances have pushed the need for greater use and sophistication of cryptography. Examples include:
  + Telegraph
  + Radio
  + The Internet
* Traditionally, cryptography was the domain of spies and the military. It was classified as a munition in the U.S. until the mid 1990s.
* Encryption is now a point of political debate.
* FBI director Christopher Wray on “going dark”: <https://www.reuters.com/article/us-usa-cyber-fbi/fbi-chief-calls-unbreakable-encryption-urgent-public-safety-issue-idUSKBN1EY1S7>
* China blocking Whatsapp: <https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html>
* Australian Prime Minister Malcolm Turnbull on encryption: <http://www.telegraph.co.uk/technology/2017/07/14/malcolm-turnbull-says-laws-australia-trump-laws-mathematics/>
* “Keys Under Doormats” article:
  + Long article: <https://academic.oup.com/cybersecurity/article/1/1/69/2367066>
* This issue came to a head in 2016 by the FBI’s unsuccessful attempt to force Apple to circumvent the encryption on their phone.
  + Timeline of the case: <http://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400/>
  + <http://fortune.com/2016/02/18/apple-fbi-opinion-makers/>
  + <http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html>
  + <https://cyberlaw.stanford.edu/blog/2016/03/cis-files-amici-curiae-brief-apple-case-behalf-iphone-security-experts-and-applied>
  + <https://www.washingtonpost.com/news/on-leadership/wp/2016/02/23/where-tech-leaders-stand-on-the-apple-vs-fbi-debate/>
  + President Obama at South by Southwest conference: <https://www.youtube.com/watch?v=FhFibpHSJFE&t=75m59s>
* Terminology:
  + What is cryptography? The etymology is Greek and means literally, “secret writing.” It is the science of creating uncrackable codes and encryption algorithms.
  + Cryptanalysis is the science of cracking uncrackable codes and algorithms. Historically, cryptography and cryptanalysis has been a cat and mouse game, with one leapfrogging the other in advances over the centuries.
  + Cryptology is an umbrella term that encompasses both cryptography and cryptanalysis.
  + Steganography is about hiding information, such as writing a letter with lemon juice for ink, or concealing text in a JPEG file. However, the data is not actually encrypted. It is freely readable if you know how/where to look.
  + More terms:
  + Plaintext: human-readable text.
  + Ciphertext: encrypted text that is not readable.
* Building blocks of encryption:
  + Transposition
    - Each character’s position changes, but it’s still the same character (i.e., its identity is unchanged).
    - Ancient example: scytale. <https://en.wikipedia.org/wiki/Scytale>
    - Another simple example is arranging text in a block and rearranging the columns:



* + Substitution
    - Each character’s position remains the same, but its identity is changed.
    - Ancient example: Caesar cipher. <https://en.wikipedia.org/wiki/Caesar_cipher>
    - c = (p + X) modulo 28, where:
      * c = ciphertext
      * p = plaintext
      * X = character to encrypt
      * mod = modulo. <https://en.wikipedia.org/wiki/Modular_arithmetic>
      * 28 = the size of the alphabet in this case, including 26 letters, a “.” and a “ ” (space).
      * One weakness of simple substitution is a frequency analysis attack. <https://en.wikipedia.org/wiki/Frequency_analysis>
      * Polyalphabetic ciphers: use multiple cipher (or substitution) alphabets (alphabets used to encrypt the plaintext).
      * Example: the Enigma machine: <https://www.youtube.com/watch?v=TYX691q2J2c>
  + Claude Shannon, pioneer of digital computing and modern cryptography, demonstrated that combining substitution and transposition, sufficiently combined, yield encrypted data that is undistinguishable from random data.
    - * Claude Shannon bio: <http://www.newyorker.com/tech/elements/claude-shannon-the-father-of-the-information-age-turns-1100100>
      * Google Doodle for 100th anniversary of his birth, 4/30/16: <https://www.google.com/doodles/claude-shannons-100th-birthday>
  + The Key
    - The workings of standard encryption algorithms are well-known. The secret is in the key, a string of bits that an algorithm uses to determine how it encrypts data.
    - The secret is in the key, not in the algorithm. This is known as Kerckhoff’s Principle. <https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle>
    - Keyspace: the set of all possible keys.
    - Bruteforcing is guessing all possible keys until you find the correct key. The larger the keyspace, the more infeasible it is to perform a bruteforce attack.
  + One-time pad. <https://en.wikipedia.org/wiki/One-time_pad>
  + Pseudo random number generator (PRNG). <https://en.wikipedia.org/wiki/Pseudorandom_number_generator>
    - Fun example: Lavalamp random number generator: <http://www.wired.com/2003/08/random/>
  + Stream cipher
    - Exclusive OR operation (XOR): <https://en.wikipedia.org/wiki/Exclusive_or>
    - By combining XOR with a PRNG, you can encrypt data.
    - Wireless access points use stream ciphers to encrypt/decrypt data they send and receive.
    - <https://en.wikipedia.org/wiki/Stream_cipher>

1. <http://money.cnn.com/2016/02/25/technology/android-apple-police-encryption/> [↑](#footnote-ref-1)