Chapter 1

Historical Introduction and the Life and Work of Claude E. Shannon

Goals, Discussion We present here an overview of historical aspects of classical cipher systems. Our objective is to give the reader a panoramic view of how the fundamental ideas and important developments fit together. This overview does not pretend to be exhaustive but gives a rough time line of development of the milestones leading to modern cryptographic techniques. The reader interested in a complete historical review is advised to consult the definitive treatise by Kahn [Kah67].

1.1 Historical Background

Cryptology is made up of two Greek words *kryptos*, meaning "hidden," and *lógos* meaning "word." It is defined [Bri19] as the science concerned with data communication and storage in secure and usually secret form. It encompasses both cryptography (from the Greek *graphia* meaning writing) and *cryptanalysis* or the art of extracting the meaning of a cryptogram.

Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century, Second Edition.
Aiden A. Bruen, Mario A. Forcinito, and James M. McQuillan.

Cryptography has a history that is almost as long as the history of the written word. Some four millennia ago (see [Kah67, p. 71]), an Egyptian scribe recorded in stone the first known hieroglyphic symbol substitution in the tomb of *Khnumhotep II*, a nobleman of the time. Although the intention in this case was to exalt the virtues of the person, rather than to send a secret message, the scribe used for the first time one of the fundamental elements used by cryptographers throughout the ages, namely **substitution**. He used unusual hieroglyphic symbols, known perhaps only to the elite, in place of the more common ones.

In substitution, the sender replaces each letter of a word in a message by a new letter (or sequence of letters or symbols) before sending the message. The recipient, knowing the formula used for the substitution – **the secret key** – is able to reconstruct the message from the scrambled text that was received. It is assumed that only the recipient and the sender know the secret key.

The other main cryptographic technique used is **transposition** (or permutation) in which the letters of the message are simply rearranged according to some prescribed formula which would be the secret key in that case.

The Greeks were the inventors of the first **transposition** cipher. The Spartans [Kah67] in the fifth century BCE, were the first recorded users of cryptography for correspondence. They used a secret device called a *scytale* consisting of a tapered baton around which was spirally wrapped either a strip of parchment or leather on which the message was written. When unwrapped, the letters were scrambled, and only when the strip was wrapped around an identically sized rod could the message be read.

Today, even with the advent of high-speed computers, **substitution** and **transposition** form the fundamental building blocks of ciphers used in **symmetric cryptography**.

To put it in a historical perspective, **asymmetric** or **public key** cryptography was not invented until the 1970s. Exactly when it was invented, or who should take most of the credit, is an issue still in dispute. Both the NSA[1] and the CESG[2] have claimed priority in the invention of public key cryptography.

Cryptography has had several reincarnations in almost all cultures. Because of the necessity of keeping certain messages secret (i.e. totally unknown to potential enemies) governments, armies, ecclesiastics, and economic powers of all kinds have been associated throughout history with the development of cryptography. This trend continues today.

The Roman General Julius Caesar was the first attested user of substitution ciphers for military purposes [Kah67, p. 83]. Caesar himself recounted this incident in his *Gallic Wars*. Caesar found out that Cicero's station was besieged and realized that without

[1] United States National Security Agency.
[2] Britain's Communications Electronics Security Group.

help, he would not be able to hold out for long. Caesar had a volunteer ride ahead, with an encrypted message fastened to a spear which he hurled into the entrenchment. Basically, Cicero was told to keep up his courage and that Caesar and his legions were on their way.

In the cipher form used by Caesar, the first letter of the alphabet "A" was replaced by the fourth letter "D," the second letter "B" by the fifth "E," and so on. In other words, each original letter was replaced by one three steps further along in the alphabet. To this day, any cipher alphabet that consists of a standard sequence like Caesar's is called a Caesar alphabet even if the shift is different from three.

Not much mention is made of the coding abilities of Augustus Caesar, the first Emperor of Rome and nephew of Julius Caesar. His cipher involved a shift of only one letter so that for the plain text (that is the original text) A was enciphered as B.

Mention of cryptography abounds in early literature: Homer's Iliad refers to secret writing. The *Kama-sutra*, the famous text book of erotics from the Indian subcontinent, lists secret writing as one of the 64 arts or yogas that women should know and practice [Kah67, p. 75]. One of the earliest descriptions of the substitution technique of encryption is given therein. One form involves the replacement of vowels by consonants and vice versa.

In Hebrew literature, there are also examples of letter substitution. The most prevalent is the **atbash** technique. Here the first and last, second and second last, and so on, letters of the Hebrew alphabet are interchanged. An example can be found in the Old Testament of the Bible. Kahn [Kah67, p. 77] cites Jeremiah 25: 26 and Jeremiah 51: 41, where the form "SHESHACH appears in place of *Babel* (Babylon)."

In Jeremiah 51: 41, the phrase with SHESHACH is immediately followed by one using "Babylon." To quote:

> How is SHESHACH taken!
>
> And the praise of the whole earth seized!
>
> How is Babylon become an astonishment
>
> Among the nations!

Through Aramaic paraphrases of the Bible, it is clear that SHESHACH is the same as Babel. With the atbash technique, the second letter of the Hebrew alphabet "b" or *beth* becomes the repeated SH or SHIN, the next to last letter in the alphabet. Similarly, the "l" of *lamed*, becomes the hard ch, or kaph of SHESHACH. Since Babylon appears below, the use of atbash here was not to actually hide the word but perhaps just a way for the scribe to leave a trace of himself in the work he was copying.

The first people to clearly understand the principles of cryptography and to elucidate the beginnings of cryptanalysis were the Arabs [Kah67]. While Europe was in the Dark Ages, Arab arts and science flourished and scholars studied methods of cryptanalysis, the art of unscrambling secret messages without knowledge of the secret key. A complete description of this work, however, was not published until the appearance of the multivolume *Subh al-a'sha* by about 1412.

European cryptology was being developed around this time in the Papal States and the Italian city-states [Kah67]. The first European manual on cryptography (c1379) was a compilation of ciphers by Gabriele de Lavinde of Parma, who served Pope Clement VII. The Office of *Cipher Secretary* to the Pope was created in 1555. The first incumbent was Triphon Bencio de Assisi. But considerably before this in 1474, Cicco Simonetta wrote a manuscript that was entirely devoted to cryptanalysis.

Cryptanalysis was to have tragic consequences for Mary, Queen of Scots. It was the decipherment of a secret message to Anthony Babington supposedly planning an insurrection against Elizabeth I [Lea96] that resulted in her tragic end. Having obtained this evidence, Sir Francis Walshingham, the head of Queen Elizabeth's secret service, sent his agent back to Fotheringay Castle, to intercept and copy more of Mary's secret messages with the result that Mary and all her coconspirators were finally arrested. As a result of the trial, all were executed but only Mary was beheaded. Walshingham later claimed that his agents had found the keys to as many as 50 different ciphers in Mary's apartments. (There has long been a conjecture that Mary was actually innocent and that the evidence was planted to remove this inconvenient rival to the English throne.)

The architect, Leon Battista Alberti born in Florence in 1404, is known as "the Father of Western Cryptology." In 1470, he published *Trattati in Cifra*, in which he described the first cipher disk. His technique led to a generalization of the Caesar cipher, using several shifted alphabets instead of just one alphabet. This gave rise to the so-called Vigenère cipher discussed in Chapter 2. (This is actually a misattribution as de Vigenère worked on auto-key systems).

In 1563, the Neapolitan, Giovanni Battista Porta published his *De Furtivis Literarum Notis* on cryptography, in which he formalized the division of ciphers into transposition and substitution.

Moving up several centuries, we find that cryptography was widely used in the American Civil War. The Federal Army [Bri97] made extensive use of transposition ciphers in which a key word indicated the order in which columns of the array were to be read and in which the elements were either plain text words or codeword replacements for plain text. Because they could not decipher them, the Confederacy, sometimes in desperation, published Union ciphers in newspapers appealing for readers to help with

the cryptanalysis. To make matters worse for the Confederate Army, the Vigenère cipher which they themselves used was easily read by the Union Army.

Kahn reports [Kah67, p. 221] that a Vigenère tableau was found in the room of John Wilkes Booth after President Lincoln was shot. Because there was actually no testimony regarding any use of the cipher, could this have been a convenient method of linking Booth and the seven Southern sympathizers with the Confederate cause?

Lyon Playfair, Baron of St. Andrews, recommended a cipher invented in 1854 by his friend Charles Wheastone, to the British government and military. The cipher was based in a digraphic[3] substitution table and was known as the *Playfair Cipher*. The main difference when compared with a simple substitution cipher is that characters are substituted two at a time. Substitution characters depend on the positions of the two plain text characters on a secret 5×5 square table (the key) whose entries are the characters of the alphabet less the letter "J."

In 1894, Captain Alfred Dreyfus of the French military was accused of treason and sent to Devil's Island, because his hand writing resembled that of an encrypted document that offered military information to Germany. To prove his innocence, the note had to be cryptanalyzed. To be certain that the decipherers' work was correct, an army liaison officer with the Foreign Ministry managed to elicit another similarly encrypted note in which the contents were known to him. The plain text then showed that Dreyfus had not written the encrypted document, but it took several more years before he was to "receive justice, re-instatement and the Legion of Honour" [Kah67, p. 262].

Early in the twentieth century, Maugborne and Vernam put forth the basis for the cipher known as the one-time pad. Although – as was proven later by Shannon – this cipher is effectively unbreakable, its use is somewhat restricted because, in practice, a random key that is as long as the message must be generated and transmitted securely from **A** to **B**. Soviet spies used this cipher, and it is said that the phone line between Washington and Moscow was protected with a one-time pad during the Cold War era.

Edward Hugh Hebern [Bri97] of the United States invented the first electric contact rotor machine. In 1915, he experimented with mechanized encryption by linking two electric typewriters together using 26 wires to randomly pair the letters. In turn, this led to the idea of rotors which could not only mechanize substitution, but also alphabet shifts as well. The function of the rotor was to change the pairing of letters by physically changing the distribution of electric contacts between the two typewriters. By 1918, he had built an actual rotor-based encryption machine.

[3] *di* meaning two, *graph* meaning character or symbol.

At about the same time (1918–1919) three other inventors, the German Arthur Scherbius, the Dutchman Hugo Koch and the Swede Arvid Damm were filing patents of rotor-based encryption machines. The Scherbius idea, which included multiple rotors, materialized in the first commercial models having four rotors, ENIGMA A and ENIGMA B in 1923. Ironically, Hebern only filed for patent protection in 1921, received one in 1924 and lost a patent interference case against International Business Machines in 1941. Later modifications to the Scherbius machine including a reflector rotor, and three interchangeable rotors were implemented by the Axis Forces during World War II.

Rotor-based machines give the possibility to implement poly-alphabetic substitution ciphers[4] with very long keys or *cycles* in a practical way. With the advantage of mechanization, the ability of widespread deployment of cryptographic stations and widespread use became a reality. This translated into a larger volume of messages (potentially all messages) being encrypted. However, the increase in traffic gave more cipher text for cryptanalysts to analyze and the probability of operators making a deadly mistake in the management of keys was multiplied.

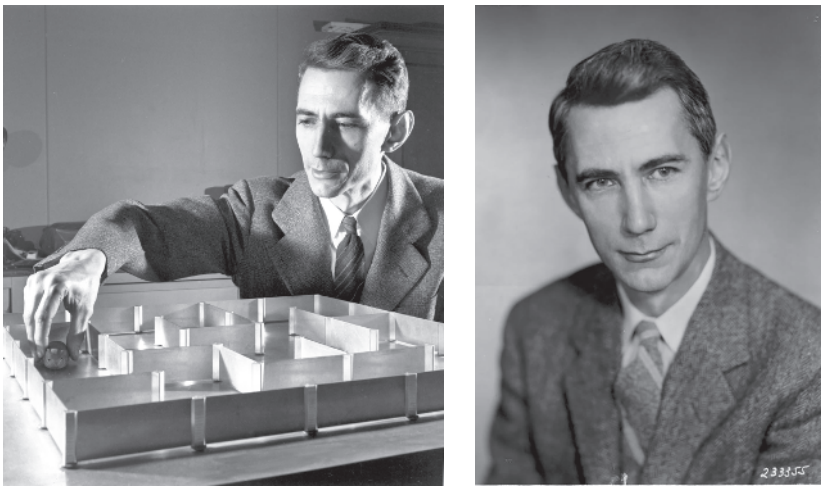
The timely breaking of the ENIGMA cipher by the Allies was due in part to inherent weaknesses in the encryption machine, mismanagement of keys by the operators and lots of mechanized, analytical work. The cipher was first broken, using only captured cipher text and a list of daily keys obtained through a spy, by the Polish mathematician Marian Rejewski. One of the important players in the mechanization of ensuing breaks was the English mathematician Alan Turing, who also contributed to the establishment of the basis for what is today called Computation Theory.

As a side note, after World War II, many of the ENIGMA machines captured by the Allies were sold to companies and governments in several countries.

Another very interesting cryptographic technique of a different kind was used by the US military in the Pacific campaign in World War II. Secret military messages were encrypted by translating them from English to the Navajo language. For decryption at the other end, of course, the Navajo was translated back into English. Some words describing military equipment did not exist in the original Navajo language, but substitutes were found. For example "tanks and planes" were described using the Navajo words for "turtles and birds." To avoid the possibility of the enemy getting a handle of the code, the whole system was committed – by means of an intensive training program – to the memory of the translators or "Code Talkers." This code was never broken.

Immediately after World War II, Shannon was publishing his seminal works on information theory. Almost simultaneously, thanks to the efforts of Ulam, von Neumann, Eckert, and Mauchly another key technological development was starting to make strident progress, the introduction of the newly invented digital computer as a mathematical tool [Coo87].

[4] A poly-alphabetic cipher uses several substitution alphabets instead of one.



(a) (b)

Figure 1.1: (a) Claude E. Shannon, Theseus, and the maze (see Section 1.4). (b) Claude E. Shannon. Source: Reused with permission of Nokia Corporation and AT&T Archives.

Because of the importance of his contributions to the issues in this book, we present here a brief biography of Shannon, before finishing the chapter with a review of modern developments (Figure 1.1).

1.2 Brief Biography of Claude E. Shannon

Claude Shannon has been described as the "father of the information age." His discoveries are everywhere. Waldrop [Wal01] gives an excellent example from the days, not so long ago, where most people listened to music on CDs, before streaming services became so popular.

> Pick up a favorite CD. Now drop it on the floor. Smear it with your fingerprints. Then slide it into the slot on the player-and listen as the music comes out just as crystal clear as the day you first opened the plastic case. Before moving on with the rest of your day, give a moment of thought to the man whose revolutionary ideas made this miracle possible: Claude Elwood Shannon.

Computers give us the power to process information. But Shannon gave us the capacity to understand and analyze information. Shannon demonstrated the unity of text, pictures, film, radio-waves, and other types of electronic communication, and showed how to use these media to revolutionize technology and our way of thinking.

1.3 Career

Shannon was born in Petoskey, Michigan in 1916. His father was a business man who later became a judge, and his mother was a high schoolteacher. As a youngster he was interested in, and became adept at, handling all kinds of contraptions such as model airplanes and boats as well as learning the workings of the telegraph system. At the age of 20, he graduated with degrees in Mathematics and Electrical Engineering from the University of Michigan.

In the summer of 1936, Claude joined the MIT Electric Engineering department as a research assistant to work on an analog computer (as opposed to our modern digital computers) under the supervision of Vannevar Bush. Bush's analog computer, called a differential analyzer, was the most advanced calculator of the era and was used mainly for solving differential equations. A relay circuit associated with the analyzer used hundreds of relays and was a source of serious study by Shannon, then, and later.

During the summer of 1937, Shannon obtained an internship at Bell Laboratories and returned to MIT to work on a Master's thesis. In September 1938, he moved to the Mathematics Department of MIT and wrote a thesis in genetics with the title *An Algebra for Theoretical Genetics* graduating in 1940 with his PhD degree in Mathematics and the S.M. degree in Electrical Engineering.

Dr. Shannon spent the academic year of 1940–1941 at the Princeton Institute where he worked with Herman Weyl, the famous group-theorist and geometer. Subsequently, he spent a productive 15 years at the Bell Laboratories in New Jersey returning to MIT in 1956, first as a visiting professor and then, in 1958, as Donner Professor of Science. This was a joint appointment between mathematics and electrical engineering. Here he did not teach ordinary courses but gave frequent seminars. According to Horgan and Claude [Hor90], he once gave an entire seminar course, with new results at each lecture!

He retired from MIT in 1978 but continued to work on many different problems including portfolio theory for the stock market, computer chess, juggling, and artificial intelligence. He died in 2001, at the age of 84 a few years after the onset of Alzheimer's Disease.

1.4 Personal – Professional

Dr. Shannon's Master's thesis [Sha40] and related publication in Transactions, American Institute of Electrical Engineers [Sha38] won him the Alfred Noble Prize along with fame and renown. The thesis has often been described as the greatest Master's thesis of all time; many feel that this may in fact understate the case.

At MIT, he was idolized by both the students and faculty. Golomb et al. [GBC+02], reports that Shannon was "somewhat inner-directed and shy, but very easy to talk to after the initial connection had been made."

In his spare time, Shannon built several items including Thrifty Roman numerical Backward-looking Computer (THROBAC) which was actually a calculator that performed all the arithmetic operations in the Roman numerical system. He also built Theseus, a mechanical mouse in 1950. Controlled by a relay circuit, the mouse moved around a maze until it found the exit. Then, having been through the maze, the mouse, placed anywhere it had been before, would go directly to the exit. Placed in an unvisited locale, the mouse would search for a known position then proceed to the exit, adding the new knowledge to its memory.

Shannon was the first to develop computerized chess machines and kept several in his house. He built a "mind-reading" machine that played the old game of penny-watching. As juggling was one of his obsessions, he built several juggling machines and worked hard on mathematical models of juggling. He was famous for riding his unicycle along the corridors at Bell Laboratories juggling all the while. On the more practical side, Shannon was also interested in portfolio management and the stock market which he connected to information theory, treating it as a noisy channel.

Over the course of his career, Dr. Shannon received umpteen awards, honors, prizes, honorary degrees, and invitations. In the end, it all became too much, and he "dropped out." To quote Waldrop [Wal01] "he turned down almost all the endless invitations to lecture or to give newspaper interviews. He didn't want to be a celebrity. He likewise quit responding to much of his mail. Correspondence from major figures in science and government ended up forgotten and unanswered in a file folder he labeled 'Letters I've procrastinated too long on.'." Dr. Shannon did attend one other Shannon lecture in Brighton, England, in 1985 (delivered by Golomb), where the shy genius created quite a stir. As Robert McEleice recalls (see [Hor90]): "It was as if Newton had showed up at a physics conference."

1.5 Scientific Legacy

Circuits

Shannon's Master's Thesis (see above and [Sha48]) was the first work to make him famous. He became intrigued by the switching circuits controlling the differential analyzer while working for Vannevar Bush. He was the first to notice that the work of a mathematics professor named George Boole in Cork, Ireland, done a century earlier, yielded the necessary mathematical framework for analyzing such circuits.

"On" and "Off" could be represented by "1" and "0." The Boolean logical operations of AND, OR correspond exactly to a circuit with two switches in series, or in parallel, respectively. He demonstrated that any logical statement, no matter how complex, could be implemented physically as a network of such switches. He also showed how the crucial Boolean decision operation could be implemented in a digital system marking the main qualitative difference between a calculator and the powerful digital computers to follow.

Cryptography

Shannon published just one paper in cryptography, namely "Communication theory of secrecy systems," [Sha49b]. Its contents had appeared in a war-time classified Bell Laboratories document which was then declassified. The beginning sentence is very revealing. It reads as follows:

> The problems of cryptography and secrecy systems furnish an interesting application of communication theory.

Indeed, this is precisely the point of view which inspired the authors of this book! We believe it is unrealistic to separate the study of cryptography from the study of communication theory embodying error-correction and information theory.

To illustrate this, Shannon points out that just as in error-correction, where the receiver tries to decode the message over a noisy channel so also, in cryptography, a receiver (this time, Eve, the eavesdropper) tries to decode the message over a noisy channel, the noise being the scrambling by the key which obfuscates the plain text to the cipher text.

In this paper, Shannon discusses at length his two famous principles of confusion and diffusion described in detail in Chapter 4. The Vernam cipher offers perfect security. We discuss perfect security in detail in Part II of the book where it is shown that, under appropriate conditions, perfect security corresponds precisely to a Latin square. Shannon's paper makes it quite clear that he was aware of this phenomenon though he did not explicitly state it.

In the paper, Shannon clearly differentiates between computational and unconditional security. Whether or not he "missed" public key cryptography is far from clear. However, in [Mas02] Massey points out that Hellman of Diffie–Hellman fame, has credited the following words from Shannon's paper as the inspiration for their discovery:

> The problem of good cipher design is essentially one of finding difficult problems .... We may construct our cipher in such a way that breaking it is equivalent to ... the solution of some problem known to be laborious.

Of course, the jury is still out, as Massey [Mas02] points out, on whether one-way functions, the foundations of public key cryptography, really exist. We refer to Chapters 3 and 4 on this point.

Shannon theory: information compression and communication.

Shannon's revolutionary paper [Sha49b] on information theory electrified the scientific world and has dominated the area of communication theory for over 50 years. No other work of the twentieth century has had greater impact on science and engineering.

First of all, Shannon unified what had been a diverse set of communications – voice, data, telegraphy, and television. He quantified and explained exactly what information means. The unit of information is the Shannon bit. As Golomb et al. [GBC+02] so elegantly puts it, this is the "amount of information gained (or entropy removed) upon learning the answer to a question whose two possible answers were equally likely, a priori."

In the above, we can think of entropy as "uncertainty" analogous to entropy in physics (which is the key idea in the second law of thermodynamics). An example would be the tossing of a fair coin and learning which turned up – heads or tails. If the coin were biased, so that the probability of a head was p (and the probability of a tail was $1-p$) with $p \neq 1/2$, the information gained, on learning the outcome of the toss, would be less than one. The exact amount of information gained would be

$$p\log(1/p) + q\log(1/q) \text{ where } q = 1-p \text{ and where we take logs to the base } 2 \qquad (1.1)$$

Note that when $p = \frac{1}{2}$ and $q = \frac{1}{2}$, this works out to be 1. However if, for example $p = 2/3$, we gain only approximately 0.918 Shannon bits of information on learning the outcome of the coin toss.

It can be mathematically proven that the only information function that gives sensible results is the appropriate generalization to a probability distribution of Formula (1.1) above. Formula (1.1) ties in to the fundamental notion of entropy (or uncertainty). There are many examples of redundancy in the English language, i.e. the use of more letters or words or phrases than are necessary to convey the information content being transmitted. As Shannon points out, the existence of redundancy in the language is what makes crosswords possible.

This redundancy can be reduced in various ways. An example is by writing acronyms such as "U.S." for "United States." When information is to be electronically transmitted, we remove redundancy by data-compression. Shannon's formula for data compression is intimately related to entropy which is in turn related to the average number of yes–no questions needed to pin down a fact. Shannon showed that it is possible to obtain a bound for the maximum compression which is the best possible. The actual technique

for compressing to that ultimate degree is embodied in the construction of the so-called Huffman codes, well known to all computer science undergraduates. Later, other compression techniques followed, leading to modern technologies used in, for example, mp3's (music compression). This part of Shannon's work is also connected to the later work of Kolmogorov on algorithmic complexity and the minimum length binary program needed for a Turing machine to print out a given sequence.

But this was only the beginning. Shannon then went on to prove his fundamental result on communication, based on entropy and the mathematical ideas delineated above. He showed that any given communications channel has a maximum capacity for reliably transmitting information which he calculated. One can approach this maximum by certain coding techniques – random coding and now turbo coding – but one can never quite reach it. To put it succinctly: *Capacity is the bound to error-free coding.* Thus, for the last 50 years, the study of error correction has boiled down to attempts to devise techniques of encoding in order to come close to the Shannon capacity. We will have much to say about this bound in Parts II and III of this book.

Shannon's work, theoretical and practical, still dominates the field and the landscape. To quote Cover in [Cov02]:

> This ability to create new fields and develop their form and depth surely places Shannon in the top handful of creative minds of the century.

Few can disagree with this assessment. Indeed, in Part III of this book, we describe protocols in cryptography and error-correction based squarely on C.E. Shannon's work in information theory.

1.6 The Data Encryption Standard Code, DES, 1977–2005

The *Data Encryption Standard*, or *DES*, was originally approved in 1977 as a block cipher algorithm that provides good cryptographic protection. Computational power has increased dramatically since 1977. DES is no longer considered to be secure. Since May 2005, it is recommended that DES no longer be used [Cen19].

The *Advanced Encryption Standard*, or *AES*, the replacement for DES, is detailed in Section 5.2.

1.7 Post-Shannon Developments

Cybersecurity

The first two decades of the twenty-first century have witnessed an explosive growth of global need for secure communications and the secure storage of data. Cybersecurity has become an area of major concern to governments and companies. Universities now offer entire degrees in cybersecurity. We discuss this more in Section 28.5.

Big data

In this big data era in which governments and private companies collect more and more information from, and make more information available to individuals in a variety of electronic formats. Along with the usual technological advances in the hardware and software of computers and networks that took place at the end of the twentieth century, there has been an increase in the variety and the uses of technology, including new devices such as smart phones, tablets, smart watches, apps on these devices, a multitude of devices from the Internet of Things (IoT), and cloud computing.

Memory (RAM)

Computers today often have 4, 8, 16, 32, or more GBs of main memory (RAM). Solid-state drives (SSDs) that are much faster (but more expensive) than hard drives (HDDs) are now prevalent in desktops and laptop computers. The memory hierarchy of a computer is discussed in Section 17.2.

Central processing unit (CPU) and graphics processing unit (GPU)

CPUs (processors, or central processing units) on desktops and laptops (and even portable devices such as smart phones) have progressed from mainly one-core processors to multicore processors with 2, 4, 8, or more cores. With multicore processors, multiple tasks can be done in parallel.

GPUs (graphics processing units), previously reserved for doing calculations to display graphics, can do some types of calculations, such as certain matrix manipulations, extremely quickly as they have many, many cores.

Moore's law

An empirical rule that has held true for a few decades is Moore's Law. In 1965, Intel cofounder Gordon Moore asserted that, **"The number of transistors incorporated in a chip will approximately double every 24 months"** (see [Int19]). For many years, the computing power of our desktop and laptop computers doubled every 18 months or so. As processor power increases, we must ensure that an adversary, Eve, who should not have the appropriate decryption keys, cannot decrypt our data and messages. This led in part to the replacement of DES with AES (see Section 1.6).

Recently, some have argued that Moore's law is dead. (See [Hea18, Sim16, Tib19], for example.) However, the performance of chips can still increase from changes in chip design. For example, multicore chips are now common-place. Multiple computations can be done in parallel (at the same time) on different cores in a chip. Other factors, such as artificial intelligence (AI), cloud computing, and quantum computing, mean that we must continue to keep our encryption algorithms up to date. The amount and types of data, some of which are very personal and/or sensitive (e.g. health records, financial records), have never been greater in quantity and sensitivity. The need for encryption using encryption algorithms that are not susceptible to attacks has never been greater.

Artificial intelligence (AI)

Artificial intelligence, AI, and machine learning are allowing cloud computing companies and even apps on phones to make predictions, such as what task should be performed next. We have progressed from having desktop and laptops to using smartphones, tablets, and smart watches, social media, cloud computing, and the IoT devices.

Smart phones

Cell phones have progressed from a basic cell phone (often a "flip phone") to Research in Motion's *BlackBerry 5810* in 2002 to Apple's first *iPhone* in 2007 to the first *Android* phone in 2008, to the smart phones of today. Phone apps allow users to video conference, watch movies, play video games, access important data, and make purchases.

Streaming – video and audio

Video and audio streaming have become so prevalent that a major portion of all Internet traffic is from streaming. We shall discuss streaming in Chapter 17.

Social media

Social media has seen exponential growth as well. For example, as of early 2019, Twitter had 126 million active daily users and Facebook had 1.2 billion daily users [Sha19]. In 2017, Facebook hit 2 billion monthly users. Yurieff notes in [Yur17] that, "It took the social network less than five years to go from 1 billion monthly users to 2 billion."

Cloud computing

Cloud computing is now extremely important, with companies offering impressive software, sometimes for free. Cloud computing providers have the ability to do some computations at much faster pace than we could with our personal devices. They have the advantage that they might have many computers at their disposal and so can use parallelism, artificial intelligence (AI) and other means to give results quickly. They can allow us to access our data from different devices from different locations in the world. Extremely important records, such as financial records and medical records, are accessible via browsers on computers and apps on phones. According to Gartner, "The worldwide public cloud services market is forecast to grow 17% in 2020 to total $266.4 billion, up from $227.8 billion in 2019 . . . ," [Gar19]. Chapter 28 deals with cloud computing.

Internet of Things (IoT)

The IoT is another major force today. It refers to any object or device that is connected to the Internet. A smart home can have many devices that can communicate with your phone, such as door bells to light bulbs to audio speakers. Amazon's Alexa is one example of IoT. In 2019, Amazon reported that over 100 million Alexa devices had been sold, [New19a]. Many IoT devices communicate by Bluetooth. The health-care field is also being transformed. As always, we need to be wary of security concerns. For example, in August 2019, *USA Today* had an article by Jefferson Graham entitled, "Sorry, readers. Your Bluetooth device is a security risk," [Gra19]. They quote Jovi Umawing, a research at Malwarebytes Labs:

> A year ago, I was on a ferry coming back from vacation and had a weird photo (a meme style image) pop up on my phone via Airdrop from a source I didn't recognize," he says. "I checked my settings, and it was open to anyone. I immediately shut it off and have left it off ever since. I turn it on to receive from people only when they are standing right in front of me."

Bluetooth has a limited range. So it is relatively safe around the home, unless there is an attacker nearby. But, in a public area, it might be best to turn it off. Graham also quotes Matt Lourens, a security engineering manager with Checkpoint software. He says,

> Another concern: shopping. Many retailers have Bluetooth beacons placed in-store to watch over you and track your location and shopping habits. Turning off Bluetooth before you enter will save your battery and keep prying eyes away from your device.

Bluetooth 5 devices have a range of up to 800 feet. (theoretically) The security of some IoT devices is of major concern. We shall discuss this further in Chapter 27 on the IoT.

Privacy concerns

Privacy and security go together. Biometrics are important as they have both applications and privacy concerns. You might use a fingerprint or facial recognition software on your phone, tablet, or computer to unlock it. Some airports now use facial recognition software to identify travelers so as to improve efficiency for processing the vast number of people that pass through an airport each day. See [Oli19] or [New19b], for example.

Security and privacy

Together, these add up to the need for security and privacy to be part of the decision-making in the development of software and hardware of devices at every stage and level. Security and privacy breaches are reported regularly on the news. Programmers must be ever vigilant to make sure that they write code in a "safe" way so as to ensure privacy and security. Will input provided to the code always be friendly, or could it be malicious? If input could arrive from an outside source (such as via the Internet), then you should assume that there will be malicious attacks. For example, for the C programming language, we recommend two wonderful books on this topic: *Secure Coding in C and C++*, second edition by Seacord, [Sea13], and *C Programming: A Modern Approach*, second edition, by King, [Kin08]. We discuss this more in Section 7.20.

Cryptography

Let us not forget cryptography. The twentieth century ended with DES, the United States Data Encryption Standard, being phased out and replaced. In 1999, Rijndael, a block

cipher developed by Joan Daemen and Vincent Rijmen was selected as the AES.[5] AES is the current standard for symmetric cryptography [NIS19b]. Chapter 5 looks at these topics.

Postquantum cryptography

Less than 20 years after the adoption of AES, the United States is preparing for a postquantum world. See [NIS19f]. We will discuss this more in Section 4.12

Blockchains

Blockchains are being used increasingly because of their immutability. In April 2020, during the COVID-19 pandemic, IBM used blockchains to help the health-care industry. In [Wei20], Weiss writes that IBM is using blockchains to connect "pop-up medical mask and equipment makers with hospitals." They quote Mark Treshock, the IBM blockchain solutions leader for IBM healthcare and life sciences as saying, "It's the immutability component. If I am a supplier and I create a profile and include my information for onboarding as a new supplier, there's a qualification process I have to go through . . . It is done to determine if they are legitimate, ethical, that they comply with required laws and, in this case, with needed FDA certifications." [Wei20]. We will discuss this more in Chapter 26.

[5] Published as Federal Information Processing Standard (FIPS) standard 197.