UNDERSTANDING ENCRYPTION & CRYPTOGRAPHY: A TECHNICAL PRIMER FOR LEGAL PROFESSIONALS

Thomas C. Reynolds*

TABLE OF CONTENTS

* Thomas C. Reynolds is a former Executive Secretary of the Export-Import Bank of the United States and an international trade and investment lawyer with over a decade of experience in export controls, sanctions, customs and national security law. He is currently a Technology Law & Policy LLM candidate at Georgetown University Law Center, and he earned his JD from Illinois Institute of Technology, Chicago-Kent College of Law in 2013, and BA from the University of Florida in 2009 (double major in Political Science and Religion). Thanks go out to Prof. Paul Ohm, Andrew Jakab, Joey Tonzi, and the rest of the GLTR staff for their helpful feedback.

INTRODUCTION

As encryption and cryptography increasingly intersect with privacy law, criminal procedure, export controls, national security, and emerging regulatory frameworks, legal professionals with a working understanding of this technology are better equipped to counsel their clients, resolve their problems, and be assured that encryption does in fact meet the confidentiality requirements of ABA professional responsibility Rule 1.6. Nevertheless, lawyers still need to take precaution in creating sophisticated passwords and applying encryption to data-at-rest, data-in-transit, and data-in-use.

With apologies to those lawyers who joined the legal field to get away from math, this article includes certain mathematical concepts underlying cryptography and encryption technology.

I. FOUNDATIONAL CONCEPTS

What is encryption? Encryption is a modern cryptographic technique to encode or scramble text and information with a key or set of keys in a way that can be unscrambled upon delivery.[1] Thinking of encryption as a causal process, it turns "plaintext" into "ciphertext."[2] This process is often used to protect sensitive information and is done through computer and telecommunications systems.

The words "cryptography" and "encryption" are often used interchangeably, but in modern times, they are slightly different concepts.[3] Cryptography has been described as the study of secure communication,[4] whereas encryption is a technique and the principal application of cryptography.[5] If you want to get even more specific, "encryption" and "decryption" are the two processes that occur at the

---

[1] *See What Is Encryption and How Does It Work?*, NORDPASS, https://nordpass.com/blog/what-is-encryption-and-how-does-it-work/ [https://perma.cc/US3G-3EUP] (last visited Nov. 1, 2025).

[2] *See* Monica Borda, *Cryptography Basics*, *in* Fundamentals in Information Theory and Coding 121, 123 (2011), https://doi.org/10.1007/978-3-642-20347-3_4; *What Is Encryption?*, IBM (July 14, 2021), https://www.ibm.com/think/topics/encryption [https://perma.cc/4G25-QR9L].

[3] Doug Bonderud, *Encryption vs. Cryptography: What's the Difference (and Why Does It Matter?)*, BARRACUDA BLOG (Aug. 1, 2025), https://blog.barracuda.com/2025/08/01/encryption-cryptography-difference [https://perma.cc/7M3A-PUHX].

[4] *Id.*

[5] *Difference between Encryption and Cryptography*, GEEKSFORGEEKS (Feb. 5, 2021), https://www.geeksforgeeks.org/computer-networks/difference-between-encryption-and-cryptography/ [https://perma.cc/EL5Q-GY9G]; *see Cryptography Basics*, *supra* note 2.

beginning and the end of the causal process, but "encryption" can be said to also include decryption.[6]

With that established, it is useful to understand how computers represent information or, "speak," and what they do with that information before getting into further detail on encryption.

A. HOW COMPUTERS STORE AND PROCESS INFORMATION

We humans speak Spanish, Tagalog, Cantonese, Igbo and other languages. Computers and algorithms, on the other hand, speak math. Every piece of digital data—text, images, video—ultimately reduces to binary: sequences of 1s and 0s. A zero or a one is called a bit,[7] and it may be useful to think of this as an on/off switch. Confusingly similar, eight bits equal one byte.[8,9] A byte is the basic processing unit that can represent a letter, a character, a number 0-9, or a symbol.[10] You may have noticed that most of your computer files have a size in kilobytes (KB), megabytes (MB), or gigabytes (GB).[11]

Before encrypting data, computers first convert it to binary code and other similar universal encoding schemes.[12] See the footnote below for how this sentence looks in binary code.[13]

---

[6] *See Difference between Encryption and Cryptography, supra* note 5.

[7] *Advanced Encryption Standard*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (U.S.) (May 9, 2023), https://doi.org/10.6028/NIST.FIPS.197-upd1.

[8] *Id.*

[9] And Mr. Two Bits equals a gator. Go Gators.

[10] *What Is a Byte & How Does It Differ from a Bit?*, LENOVO US (Nov. 1, 2025), https://www.lenovo.com/us/en/glossary/what-is-a-byte/ [https://perma.cc/7PMC-9WUN] (last visited Nov. 1, 2025).

[11] If you are reading this from the future, maybe personal files are now in gigabytes (GB), terabytes (TB), petabytes (PB), or more.

[12] For example, the American Standard Code for Information Interchange (ASCII) is a character encoding standard that uses numbers 0 to 127 to represent standard keyboard symbols, letters and functions. An 8-bit byte can also represent a 2-digit hexadecimal.

[13] 01010011 01100101 01100101 00100000 01110100 01101000 01100101 00100000 01100110 01101111 01101111 01110100 01101110 01101111 01110100 01100101 00100000 01100110 01101111 01110010 00100000 01101000 01101111 01110111 00100000 01110100 01101000 01101001 01110011 00100000 01110011 01100101 01101110 01110100 01100101 01101110 01100011 01100101 00100000 01101100 01101111 01101111 01101011 01110011 00100000 01101001 01101110 00100000 01100010 01101001 01101110 01100001 01110010 01111001 00100000 01100011 01101111 01100100 01100101 00101110. CONVERT BINARY.COM, https://www.convertbinary.com, [https://perma.cc/2XNL-35LM].

B. MATHEMATICAL FOUNDATIONS OF ENCRYPTION

Once information is translated into a language that a computer can "understand," there are at least three mathematical concepts that underpin virtually all modern encryption systems.

First, modular arithmetic operates on the same principle as a clock or our time system. That round, analog clock at the front of a classroom only shows numbers one through twelve, even though we have twenty-four hours in a day. We tell time on a modulus 12 (or "mod 12") system. So, when it's 15:00 in military time, we divide the hour (15) by the modulus (12),[14] get 1 and a fraction of 12, and that remainder (3) is the hour of the day (3 pm), à la long division. This "wrapping around" feature allows encryption algorithms to more efficiently factor large numbers and properties.[15]

It also demonstrates another feature of encryption: the importance of the "key" in encrypting and decrypting information. In that previous example, 3 and 15 can be considered different numbers (one is 3, the other is 15), *but for* the "key" or modulus of 12 (therefore, both 3 o'clock and 15 o'clock are both 3 o'clock). Particularly with much larger numbers, it would be difficult to identify this without the "key" of 12.

Second, prime numbers are an important mathematical feature found in encryption. Prime numbers are natural numbers greater than 1 that are only divisible by 1 and themselves.[16] For example, 2, 3, 5, 7, 11, 13, 17, 19, and 23 are all prime. Composite numbers, on the other hand, are divisible by at least one number other than 1 and itself. For example, 4, 6, 8, 9, 10, 12, and 15[17] are all examples of composite numbers.[18]

Prime numbers are mathematically complicated and are used to generate key pairs in certain encryption algorithms.[19] When multiplying two large prime numbers, one gets a large composite number (take for example, 12,331,093 x 4,294,967,291 = 5.296 x 10^{16}). If one only has the large composite number, factoring it back

---

[14] 15/12 = 1 & 3/12ths.

[15] *Modular Arithmetic*, GEEKSFORGEEKS (May 4, 2020), https://www.geeksforgeeks.org/engineering-mathematics/modular-arithmetic/ [https://perma.cc/K52N-X7DN].

[16] *Prime Numbers*, BRILLIANT, https://brilliant.org/wiki/prime-numbers/ [https://perma.cc/T3NN-MXMC] (last visited Nov. 21, 2025).

[17] Even numbers (except 2) are all composite numbers, but some odd numbers are also composite numbers.

[18] All are divisible by 2, except 15, which is divisible by 3.

[19] *See What Is Encryption?*, *supra* note 1.

into the two prime numbers is an intricate mathematical problem which provides security, even with high-end computers.[20]

Third, the last foundational concept I will provide here is that of "XOR (Exclusive OR)." XOR is a logic operation applied to bits or binaries, which is fundamental to encryption. The XOR logic gate outputs 1 (true) if the combination of two input bits (plaintext and a key) is dissimilar, and outputs 0 (false) if the two inputs are similar. The following truth table provides an example of this function.

Ciphertext/Plaintext	**1**	**0**
0	1	0
1	0	1

Once XOR is applied to the plaintext using the key (for example, "password") the key will be broken down into bits of 0 and 1, and this will "scramble" the plaintext or data meant to be protected into the ciphertext.[21] If the key is shorter than the message to be encrypted, as so many messages or pieces of data are, the key can be repeated to fit the length of the message. And if you know the key, XOR is also reversible in order to decrypt data.

Summary	
1. Modular Arithmetic	e.g. a circular 12-hour analog clock
2. Prime Numbers	huge numbers that cannot be divided by any other number than itself and one
3. XOR	a logic game

II. THE FUNDAMENTAL APPROACHES

Encryption approaches are typically divided into two categories based on how they handle keys: symmetric encryption and

[20] *Prime Numbers in Cryptography*, GEEKSFORGEEKS (Feb. 16, 2024), https://www.geeksforgeeks.org/maths/why-prime-numbers-are-used-in-cryptography/ [https://perma.cc/ZAC8-RY7J].

[21] *See* Administrator, *XOR Encryption Algorithm,* 101 COMPUTING (Nov. 28, 2020), https://www.101computing.net/xor-encryption-algorithm/ [https://perma.cc/6S4T-K23Y].

asymmetric encryption.[22] While technically not encryption, "hashing" is a cryptographic technique that is also important.[23] And looking to the future, quantum cryptography will be a game-changer.

Symmetric encryption uses the same key for both encryption and decryption, like a house key that both locks and unlocks your door.[24] These systems are fast and efficient, making them ideal for encrypting large amounts of data.[25] The challenge lies in key distribution: how do two parties share the secret key without an eavesdropper intercepting it?[26]

Asymmetric encryption solves the key distribution problem by using a pair of mathematically related keys.[27] A public key encrypts data while a different key that remains private decrypts it.[28] Think of a mailbox where anyone can drop letters through the slot, but only the owner possesses the key to open it. Each user generates a key pair, freely distributing the public key while keeping the private key secret.[29] This innovation, though slower computationally, revolutionized secure communications by eliminating the need to share secret keys in advance.

Hashing is a cryptographic technique that, unlike symmetric encryption and asymmetric encryption, is not meant to be reversible. It serves functions where a one-way encoding works perfectly fine or is preferable. Examples include password storage, digital signatures, and data integrity validation.

The basic difference between traditional cryptography and quantum cryptography is that the former is based in math and geometry, whereas the latter is based on the laws of physics. Principles such as the Heisenberg Uncertainty Principle[30] and

---

[22] *Difference Between Symmetric and Asymmetric Key Encryption*, GEEKSFORGEEKS (Jan. 29, 2020), https://www.geeksforgeeks.org/computer-networks/difference-between-symmetric-and-asymmetric-key-encryption/ [https://perma.cc/EJT4-TX2Q].

[23] *See Difference between Hashing and Encryption*, GEEKSFORGEEKS (Jan. 11, 2021), https://www.geeksforgeeks.org/computer-networks/difference-between-hashing-and-encryption/ [https://perma.cc/X99K-NJ9G].

[24] *Difference Between Symmetric and Asymmetric Key Encryption, supra* note 22.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] The Heisenberg Uncertainty Principle postulates that the position and the velocity of an object cannot be measured exactly, at the same time.

quantum entanglement[31] form the basis of quantum encryption, which is by and large still in developmental stages. Nevertheless, quantum cryptography products such as key generators are already on the market and can be used to supplement traditional encryption techniques.

III. SYMMETRIC ENCRYPTION EXPLAINED

Symmetric encryption is the technique that uses the same key to encrypt and decrypt ciphertext.[32] To do this, symmetric encryption primarily uses two techniques that combine the plaintext and the key: substitution and transposition and does so either bit-by-bit or by blocks of bits.[33] Using the popular Advanced Encryption Standard (AES) symmetric encryption algorithm as an example, AES is a block cipher that divides messages into 128-bit blocks or 16 bytes or characters at a time.[34] Then through multiple rounds of transformations, it encrypts each block. Each round applies four operations[35] that systematically scramble the data: Round 1 substitutes each byte from the plaintext with a different byte according to a predetermined lookup table and creates a matrix like the one below.[36]

b0	b1	b2	b3
b4	b5	b6	b7
b8	b9	b10	b11
b12	b13	b14	b15

Round 2 is called "ShiftRows" because it scrambles or shifts rows 2 through 4 according to specific rules.

Britannica Editors, *Uncertainty Principle*, BRITANNICA (Dec. 5, 2025), https://www.britannica.com/science/uncertainty-principle.

[31] Einstein described quantum entanglement as "spooky action at a distance." It is the phenomenon where particles that were once connected always stay connected, regardless of how far apart they are in time and space. *What Is Quantum Entanglement?*, NASA (Oct. 30, 2024), https://science.nasa.gov/what-is-the-spooky-science-of-quantum-entanglement/ [https://perma.cc/KUE6-42GU].

[32] *Symmetric Key Cryptography*, GEEKSFORGEEKS (May 1, 2024), https://www.geeksforgeeks.org/computer-networks/symmetric-key-cryptography/ [https://perma.cc/EDD3-SRG3].

[33] *Id.*

[34] *Advanced Encryption Standard (AES)*, GEEKSFORGEEKS (Oct. 15, 2021), https://www.geeksforgeeks.org/computer-networks/advanced-encryption-standard-aes/ [https://perma.cc/6BFC-8BPD].

[35] *Id.*

[36] This round is called "SubBytes." *Id.*

b0	b1	b2	b3
b5	b6	b7	b4
b10	b11	b8	b9
b15	b12	b13	b14

Round 3: Now it's the columns' turn.[37] The columns b0 through b3 (which you may notice above remained the same) are multiplied by a specific matrix which scrambles the position of each byte in the column. Finally, round 4: "Add Round Key" adds a key unique to the round that is mathematically related to the cipher key, XORs it with the result of round 3, and finally, starts the next round unless this process has already been repeated 10, 12 or 14 times (depending on the key size).[38]

After 10 or more rounds of these four operations, 16 bytes of plaintext become 16 bytes of encrypted gibberish. The process repeats for each subsequent block and for the same number of rounds. To decrypt the text with the same key, the algorithm applies inverse operations in reverse order, unwinding the transformation to recover the original message.

The security of AES rests on an avalanche effect: changing a single bit of input or the key produces dramatically different output. Without knowing the key, an attacker using a brute force[39] search would need to try 2^^128 (or more) possible keys[40]—an infeasible task. AES-256 is the rockstar of symmetric encryption. A USB drive may use it to encrypt data-at-rest that is saved on it. Communications via email, Voice-over-IP (VoIP), and others may use it to encrypt the data-in-transit over their communication lines or to provide security to a wi-fi network or over a virtual private network (VPN).

IV. ASYMMETRIC ENCRYPTION EXPLAINED

Asymmetric encryption on the other hand uses two keys: one to encrypt and another to decrypt.[41] It is particularly suited for data-in-transit because the key to encrypt data is made public, whereas the

---

[37] This round is creatively called "MixColumns." *Id.*

[38] *Id.*

[39] *Brute Force Attack*, GEEKSFORGEEKS (Jan. 27, 2020), https://www.geeksforgeeks.org/computer-networks/brute-force-attack/ [https://perma.cc/NXZ5-J8GC].

[40] *Symmetric Key Cryptography*, *supra* note 32 (This number is: 340,282,366,920,938,463,463,374,607,431,768,211,456 or approximately 340 undecillion).

[41] *Asymmetric Key Cryptography*, GEEKSFORGEEKS (Mar. 25, 2024), https://www.geeksforgeeks.org/computer-networks/asymmetric-key-cryptography/ [https://perma.cc/Z348-XA2U].

key to decrypt is kept private.[42] This method typically takes longer and creates larger file sizes but is more secure than symmetric encryption.[43] Crucially, it solves the question on how to securely share keys. Since the key to encrypt data is public, the algorithm can pull the public key of the intended destination, use it to encrypt the data, send it, and then the recipient will already have the secret decryption key. Sometimes, asymmetric encryption is used in conjunction with symmetric encryption, particularly if using the asymmetric public key encryption solely to establish a key for the symmetrically encrypted message.[44] The trick in all this is in the math.

A. RSA EXPLAINED (CLASSIC APPROACH)

Using the classic public key system, the Rivest-Shamir-Adleman asymmetric encryption algorithm (or RSA), as an example, the first important step is the key generation. This step proceeds as follows:

First, Anne (or the algorithm) selects two large random prime numbers, p and q. Anne multiplies them to get n (i.e., $n = p \times q$).[45] This product, n, becomes half of the public key[46] and half of the private key.[47] While multiplying is easy, factoring or dividing n back into p and q should be computationally difficult or infeasible with current technology. This is an important part of the security that RSA provides.

Next, for the private key, Anne uses those same prime numbers to calculate $\varphi(n)$ ($\varphi(n) = (p\text{-}1)(q\text{-}1)$).[48] And to complete the public

---

[42] *Id.*

[43] *Id.*

[44] MAEVE COATES WELSH, ELLIPTIC CURVE CRYPTOGRAPHY 6 (2017), https://math.uchicago.edu/~may/REU2017/REUPapers/CoatesWelsh.pdf [https://perma.cc/JR9J-G7RY].

[45] *RSA Encryption*, BRILLIANT MATH & SCIENCE WIKI, https://brilliant.org/wiki/rsa-encryption/ (last visited Nov. 16, 2025) [https://perma.cc/HX4W-CQHE].

[46] *See id.*

[47] *Cryptography and Its Types*, GEEKSFORGEEKS (July 8, 2019), https://www.geeksforgeeks.org/computer-networks/cryptography-and-its-types/ [https://perma.cc/G5AG-DXZR].

[48] *See RSA Encryption*, *supra* note 45.

key, Anne chooses a number e that is relatively prime[49] to $\phi(n)$.[50] After some modular arithmetic to find the modular inverse d of a number related to e,[51] d is kept secret and completes the private key.[52] In order to figure out d, one would need to know $\varphi(n)$, which requires knowing p and q, which requires factoring n (which is half of the public key and the private key).

To encrypt a message M, the algorithm uses the two halves of the public key, e & n, to create the ciphertext, $M^e \bmod n$.[53] To decrypt the message, the encryption can be reversed with the two parts of the private key, n & d, by calculating $C^d \bmod n$ (where C is the ciphertext).[54]

Given the high security in this asymmetric encryption algorithm, RSA is used to secure online banking, e-commerce, and secure communications.[55]

B. Elliptic Curve Cryptography (Modern Approach)[56]

Another popular asymmetric algorithm is the Elliptic Curve Cryptography (ECC), which is a modern approach. Instead of relying on huge prime numbers like RSA does, ECC uses geometric figures (ellipses) to achieve comparable security with a smaller key size.[57]

Elliptic Curve Cryptography (ECC) achieves equivalent security with much smaller keys by replacing multiplication and factoring with geometric operations on algebraic curves.[58] An elliptic curve is usually created by a function $y^2 = x^3 + Ax + B$,[59] with a "generator

---

[49] Two positive integers are relatively prime if their greatest common divisor is 1. For example, 16 & 7 are relatively prime to each other. Neither integer needs to be a prime number in the absolute sense. *Relatively Prime,* Brilliant Math & Science Wiki, https://brilliant.org/wiki/relatively-prime/ [https://perma.cc/ZPS9-UVBZ] (last visited Nov. 17, 2025).

[50] *See RSA Encryption*, *supra* note 45. A commonly used number is 65,537 ($2^{16}+1$).

[51] $(e \times d) \bmod \varphi(n) = 1$. *Cryptography and Its Types*, *supra* note 47.

[52] *Id.*

[53] *RSA Algorithm in Cryptography*, GeeksforGeeks (Apr. 22, 2017), https://www.geeksforgeeks.org/computer-networks/rsa-algorithm-cryptography/ [https://perma.cc/YQX8-JRJS].

[54] *Id.*

[55] *Id.*

[56] *Blockchain - Elliptic Curve Cryptography*, GeeksforGeeks (Nov. 15, 2022), https://www.geeksforgeeks.org/ethical-hacking/blockchain-elliptic-curve-cryptography/ [https://perma.cc/PSJ6-APEH].

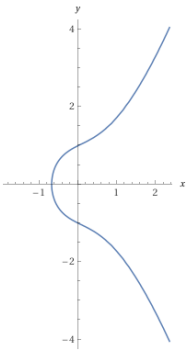
[57] *Id.;* Arup Guha, *Elliptic Curves (for Use in Cryptography),* https://www.cs.ucf.edu/~dmarino/ucf/cis3362/lectures/newlecs/EllipticCurves.pdf [https://perma.cc/NJ4P-C7K5] (last visited Jan. 6, 2026).

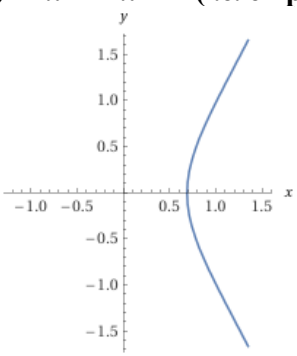
[58] *Blockchain – Elliptic Curve Cryptography*, *supra* note 56.

[59] Welsh, *supra* note 44, at 1.

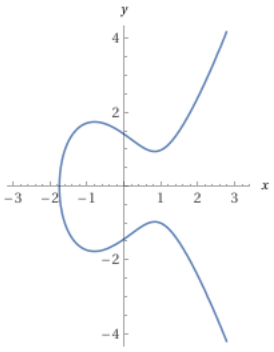
point" or base point on the graph to create a finite field to keep things compact.[60]

Examples of $y^2 = x^3 + Ax + B$ (i.e. ellipses)





Ex. $y^2 = x^3 + x + 1$ Ex. $y^2 = x^3 + x - 1$



Ex. $y^2 = x^3 - 2x + 2$

Using the chosen graph, the private key in this type of asymmetric encryption (the key to decrypt) is a random integer within the defined field around the elliptic curve.[61] The public key (the key to encrypt) is then derived using scalar multiplication that multiplies the base point by the private key,[62] which results in points on the elliptic curve on an (x, y) coordinate.[63] Because the private key is just one point on the curve, this allows a 256-bit ECC key (i.e. a mere 32 bytes or characters) to be the equivalent of a 3,072-bit RSA key (i.e. 384 bytes).[64]

ECC is often used in conjunction with symmetric encryption to secure the key exchange rather than directly for encryption/decryption of data.[65] It can also be used to create a digital

---

[60] *Blockchain - Elliptic Curve Cryptography*, *supra* note 56.
[61] *Id.*
[62] *Asymmetric Key Cryptography*, *supra* note 41.
[63] *Blockchain - Elliptic Curve Cryptography*, *supra* note 56.
[64] *Id.*
[65] *Asymmetric Key Cryptography*, *supra* note 41.

signature[66] that verifies the authenticity of a document and for the related concept of non-repudiation—the digital evidence of a participant's receipt of a conversation or document.[67] You can also find ECC in the blockchain.[68]

V. HASH FUNCTIONS AND DIGITAL SIGNATURES EXPLAINED

While hashing technically isn't encryption, it is a type of cryptographic function that is frequently used in a similar way for data protection purposes. [69] Whereas encryption should be able to be decrypted with the right key, hashing is a one-way street meant to create a digital fingerprint.

SHA-256 is one of the most prominent hashing standards.[70] It processes any input, small or large,[71] and outputs a 256-bit hash value.[72] When facing a given text, a good hash function will transform the text into unique hashed text by uniformly breaking down the plaintext components into a "Hash Table" of simplified numbers or characters using modular functions and anti-collision techniques without overburdening the Hash Table.[73]

This construction underpins secure web browsing (TLS/SSL), integrity verification and digital signatures.[74] For passwords, a system can then compare those gibberish texts instead of seeing the

---

[66] *What Is Public Key Encryption?,* IBM, (June 20, 2025), https://www.ibm.com/think/topics/public-key-encryption [https://perma.cc/VHU7-JSQC].

[67] *What Is Non Repudiation?*, GEEKSFORGEEKS (Apr. 23, 2024), https://www.geeksforgeeks.org/computer-networks/what-is-non-repudiation/ [https://perma.cc/F9R7-XB28].

[68] *Blockchain - Elliptic Curve Cryptography*, *supra* note 56.

[69] *See Difference between Hashing and Encryption*, *supra* note 23.

[70] *SHA-256 and SHA-3*, GEEKSFORGEEKS (Mar. 20, 2024), https://www.geeksforgeeks.org/computer-networks/sha-256-and-sha-3/ [https://perma.cc/84VC-X6AL].

[71] "This sentence is longer than 256 bits in order to test whether the output is 256 bits long" can be hashed into 27126434c3dad5fbbe05a81bbd13c208c972f0d573a5ff9534a0e73c237035f9. *SHA-256 Hash Generator*, Hash Generator https://hash-generator.com/sha-256 [https://perma.cc/5U29-YBVF] (last visited Jan. 6, 2026).

[72] *SHA-256 and SHA-3*, *supra* note 70.

[73] *See Introduction to Hashing*, GEEKSFORGEEKS (July 4, 2022), https://www.geeksforgeeks.org/dsa/introduction-to-hashing-2/ [https://perma.cc/75HL-QD2H].

[74] *Generating an SHA-256 Hash From the Command Line*, GEEKSFORGEEKS (Dec. 28, 2022), https://www.geeksforgeeks.org/linux-unix/generating-an-sha-256-hash-from-the-command-line/ [https://perma.cc/D6E6-594W].

actual password itself. This is why hacks targeting banks sometimes have compromised password data, but the hackers may not have actually received any plaintext passwords.

VI. QUANTUM ENCRYPTION EXPLAINED

While traditional encryption relies on computational difficulty, quantum cryptography uses physics itself to secure communications. However, quantum cryptography remains fairly theoretical. The most prominent use is in quantum key distribution (QKD) accompanied by traditional methods of encrypting the message[75] and can be based on either the Heisenberg Uncertainty Principle[76] or quantum entanglement.[77]

The BB84 protocol[78] illustrates the approach based on the Heisenberg Uncertainty Principle. Say Anne prepares photons[79] in quantum states representing 0s and 1s, randomly choosing between two polarization bases for each photon (straight up and down/sideways left to right, or diagonal one way/diagonal the other way).[80] She sends these photons to Bob through a quantum channel. Bob measures each photon, randomly selecting his measurement basis. If he happens to select the right basis, quantum mechanics law would allow him to read the results. If he does not select the right basis, the message would be effectively destroyed.[81]

Bob then publicly announces which bases he used, but not the results, and typically only discloses a third of the message.[82] If Anne confirms, Anne & Bob discard those bits and the remainder becomes their secret key. These matching bits become their shared secret key

---

[75] *Quantum Cryptography*, GEEKSFORGEEKS (Jan. 9, 2019), https://www.geeksforgeeks.org/computer-networks/quantum-cryptography/ [https://perma.cc/2VQY-ZT2J].

[76] The Heisenberg Uncertainty Principle postulates that the position and the velocity of an object cannot be measured exactly, at the same time. Britannica Editors, *Uncertainty Principle*, BRITANNICA, https://www.britannica.com/science/uncertainty-principle.

[77] *Quantum Cryptography*, *supra* note 75. .

[78] Not to be confused with the BB-8 droid in Star Wars.

[79] Photons are packets of light and elementary particles with no mass or electrical charge that behave like both particles and waves. Anne Helmenstine, *What Is a Photon? Definition and Facts*, SCIENCENOTES.ORG (Dec. 14, 2022), https://sciencenotes.org/what-is-a-photon-definition-and-facts/ [https://perma.cc/8SXS-QHCH].

[80] *See* Marin Ivezic, *Quantum Key Distribution (QKD) and the BB84 Protocol*, POSTQUANTUM.COM (Apr. 13, 2020), https://postquantum.com/post-quantum/qkd-bb84/ [https://perma.cc/THV4-C8EL].

[81] *Id.*

[82] *Id.*

for the next message using traditional encryption. The comparison also allows them to potentially detect an intrusion because under the laws of quantum mechanics, an intrusion requires a measurement of the stream of photons. But measuring the photons collapses the state (e.g. a photon polarized at a 26°), introducing errors in the final accounting between Anne & Bob.[83] If Bob randomly chose the wrong alignment or an intruder disturbed the transmission, they try again.

Quantum cryptography can thus be more secure, but it is also currently slow and expensive, with the communication range being fairly limited.[84]

VII. CONCLUSION

Encryption and cryptography are important parts of modern society. Clients use them to secure data and information, and their lawyers have an ethical duty to keep client information confidential. These security protocols also play an important role in various types of law, including national security, privacy, and even in the rules of evidence by laying a foundation and establishing a chain of custody.

Symmetric encryption, asymmetric encryption, hashing, and quantum encryption are four of the most important cryptographic applications today and in the near future. I hope this Tech Explainer demystified these applications and also established the importance of enabling encryption on hard-drives, cloud applications, communication channels, etc., as well as the importance of using longer and more complicated passwords to create stronger keys.

---

[83] *See id.*

[84] *Differences between Classical and Quantum Cryptography*, GEEKSFORGEEKS (Apr. 29, 2019), https://www.geeksforgeeks.org/computer-networks/differences-between-classical-and-quantum-cryptography/ [https://perma.cc/M25Y-ZGJT].