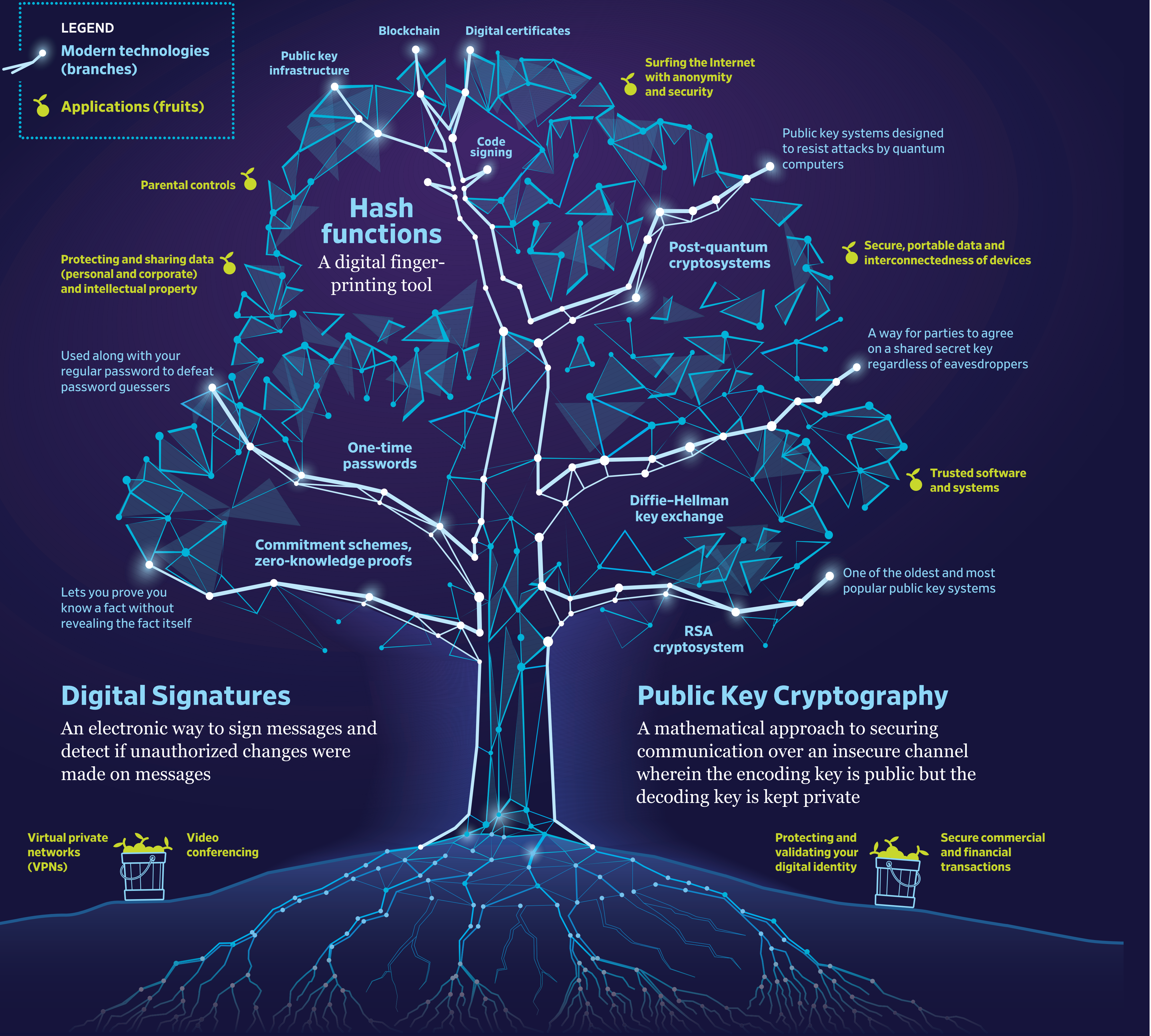
The Mathematics of Internet Security

The Internet is a transformative network that is an integral part of our daily lives—but, unfortunately, its use involves many security challenges. With roots in abstract mathematics, some new and some very old, a tree of technologies (cryptosystems and authentication schemes) has grown to meet evolving threats. As users of the Internet, we routinely enjoy this tree's fruits and may not appreciate their origins.

Mathematics helps protect against evolving threats

- Bots and fake accounts
- Corporate espionage
- Malicious websites
- Financial fraud and hacking
- Identity theft
- Intellectual property theft
- Malware or spyware
- Phishing, trojans, and spam
- Stolen medical records



LEGEND

Modern technologies (branches)

Applications (fruits)

Blockchain

Digital certificates

Public key infrastructure

Surfing the Internet with anonymity and security

Code signing

Public key systems designed to resist attacks by quantum computers

Parental controls

Hash functions

A digital fingerprinting tool

Post-quantum cryptosystems

Protecting and sharing data (personal and corporate) and intellectual property

Secure, portable data and interconnectedness of devices

A way for parties to agree on a shared secret key regardless of eavesdroppers

Used along with your regular password to defeat password guessers

One-time passwords

Trusted software and systems

Diffie-Hellman key exchange

Commitment schemes, zero-knowledge proofs

One of the oldest and most popular public key systems

Lets you prove you know a fact without revealing the fact itself

RSA cryptosystem

Digital Signatures

An electronic way to sign messages and detect if unauthorized changes were made on messages

Public Key Cryptography

A mathematical approach to securing communication over an insecure channel wherein the encoding key is public but the decoding key is kept private

Virtual private networks (VPNs)

Video conferencing

Protecting and validating your digital identity

Secure commercial and financial transactions

Intractable computations

Cryptosystems aim to force an eavesdropper to solve intractable problems that often involve large numbers while the intended users simply verify known solutions. These intractable problems include finding the shortest vector in a lattice (1998) and decoding random linear codes (1978).

Algebra on elliptic curves

An elliptic curve over a finite field is a simplified solution set to a polynomial equation. In the 1980s, it was noticed that translating cryptographic algorithms into this setting allowed the use of smaller numbers while achieving the same level of security.

Concentration inequalities

Concentration inequalities, such as Bernstein's Inequalities (ca. 1930), are used to analyze the security of cryptosystems. These limit the chances that a random variable, a quantity that changes upon repeated measurements, is significantly different from what is expected.

Computational number theory

This field studies ways to use computers to solve arithmetic problems. The RSA cryptosystem uses the unique prime factorizations of numbers (ca. 300 BCE) and Euler's theorem (1763), and its security relies on the obstacle of identifying such factors for select large numbers.

High-dimensional geometry

Structured collections of points called lattices are useful settings for cryptosystems and problems in cryptology. Lattices in high dimensions were used to create the first proof-of-concept system for homomorphic encryption (2009).

[Internet Security Is Rooted in Mathematics]

NATIONAL ACADEMIES *Sciences Engineering Medicine*

This information is from Illustrating the Impact of the Mathematical Sciences, available online at http://nas.edu/illustrating-math.