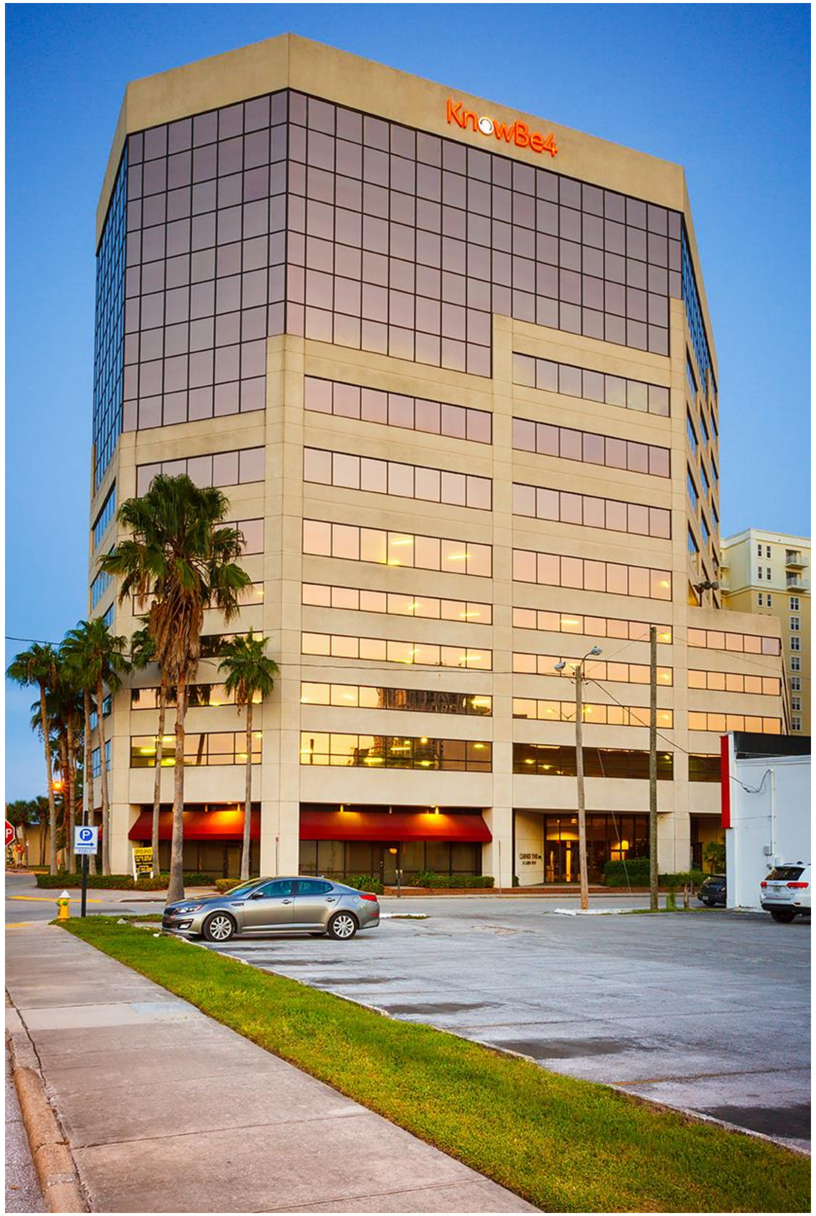
KnowBe4
Human error. Conquered.

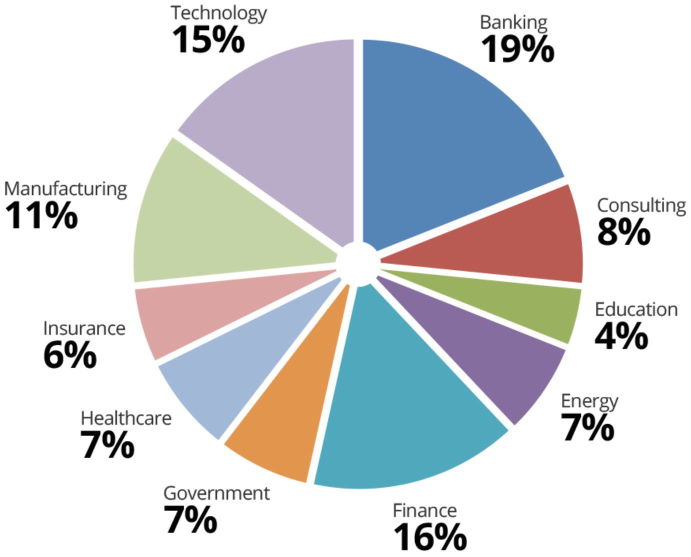
The Quantum Break is Coming
Will You Be Ready?

Roger Grimes
Data-Driven Defense Evangelist,
KnowBe4, Inc.
rogerg@knowbe4.com



KnowBe4, Inc.

- The world’s most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering



Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

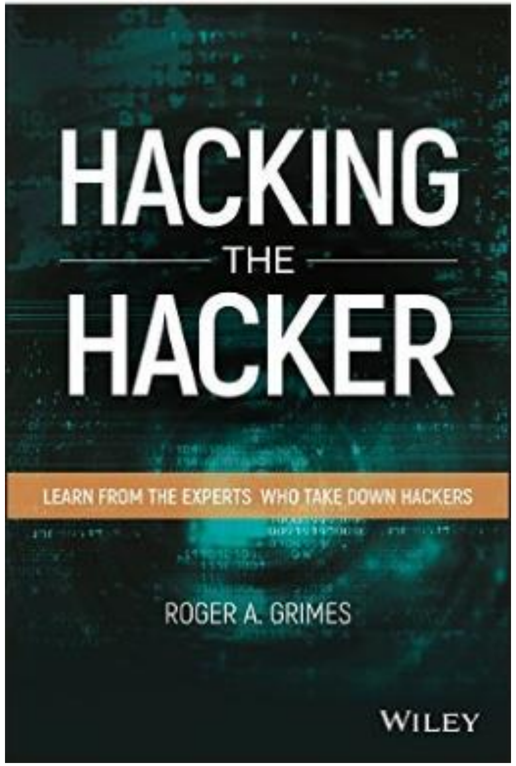
About Roger

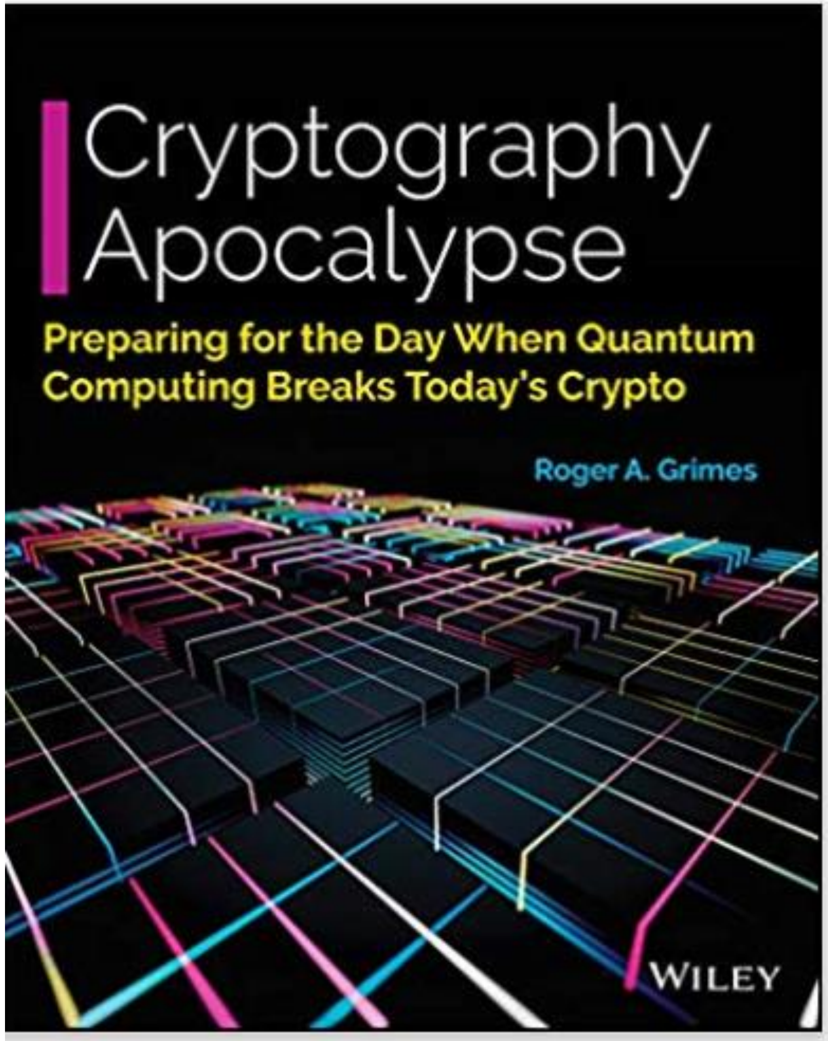
- 30-years plus in computer security
- Written 12 books and over 1000 magazine articles
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Member of Cloud Security Alliance (CSA) Quantum working group
- Consultant to hundreds of the world's largest and smallest companies and militaries for decades
- Previously worked for Foundstone, McAfee, Microsoft
- InfoWorld and CSO weekly security columnist 2005
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

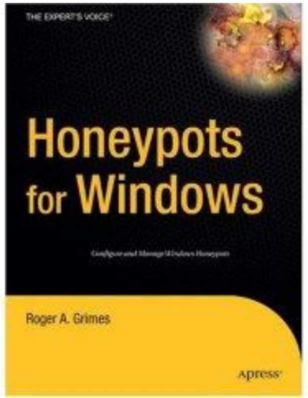
Certifications passed include:

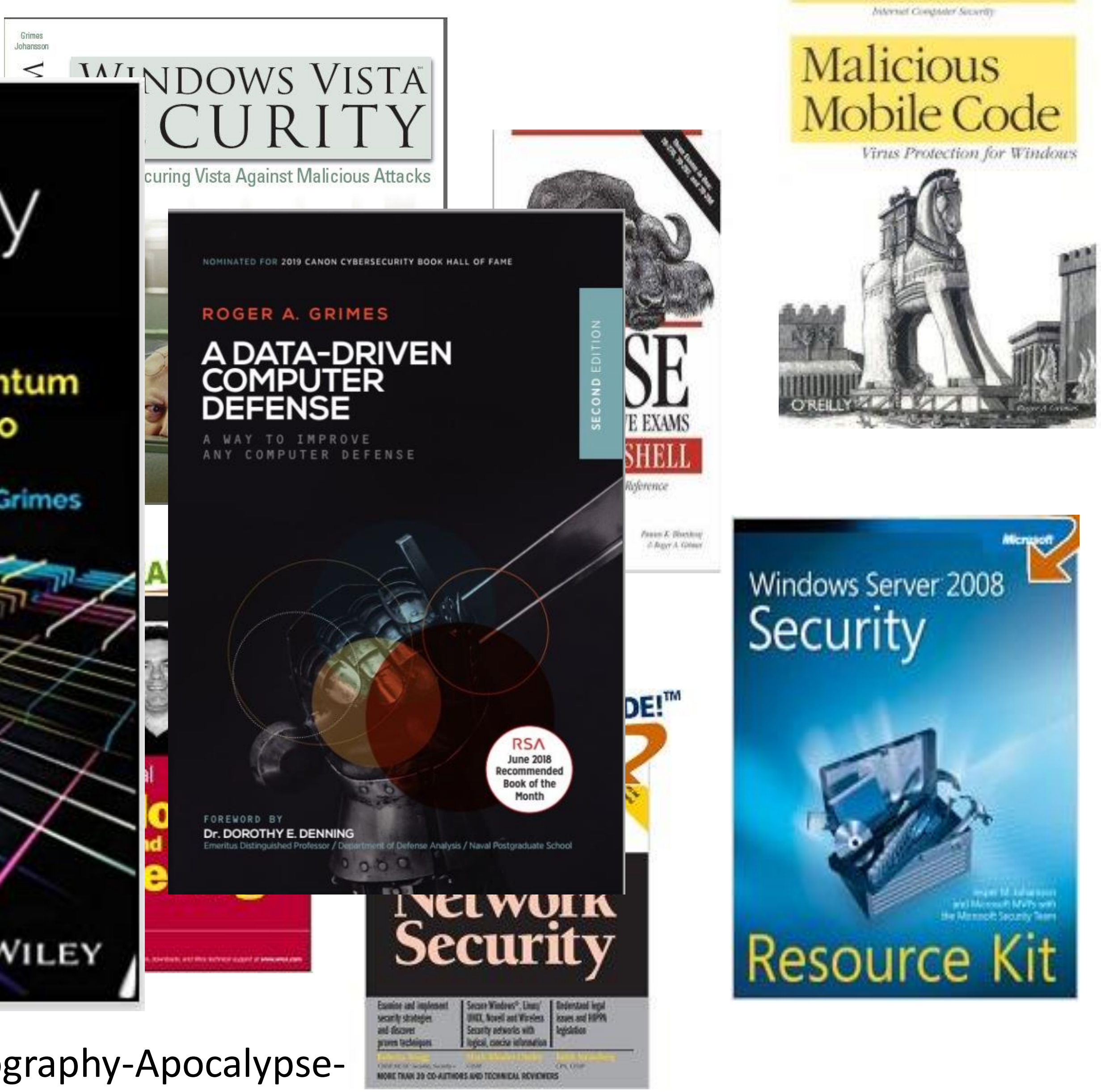
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

Roger's Books









https://www.amazon.com/Cryptography-Apocalypse-Preparing-Quantum-Computing/dp/1119618193

Quantum Crypto Break

Summary

- Quantum computers are soon likely to break most traditional public key crypto and every secret it protects
  - Ex: RSA, DH, ECC, ElGamal, PKI, digital certificates, digital signatures, TLS, HTTPS, VPNs, WiFi protection, smartcards, HSMs, crypto-currencies, two-factor authentication which relies on digital certificates (e.g. FIDO keys, Google security keys, etc.), digital signatures, etc.
  - And weaken many other types (symmetric, hashes, random number generators, etc.)

Today’s Presentation

- A Few Quantum Facts
- Quantum Computing
- Quantum Crypto Break
- How to Prepare

Quantum Mechanics

- Simply the way all things work, but only easily seen at the sub-molecular level
- Can be more readily seen with elementary particles (e.g. electron, photon, quark, etc.)
- Many "strange and weird" behaviors we have proven absolutely exist, but we don't always know how or why they occur
- Quantum behavior seems very counterintuitive to what we thought we knew of the universe before, using "classical" physics and gravity
- Einstein was an early discoverer (got his only Nobel prize for it), but got so weirded out by the unexplainable strangeness (e.g. "spooky action at a distance" and "god doesn't throw dice") that he couldn't wholly believe in it. Went to his grave not fully believing in it.
- Quantum was later proven to be real and underlying all things. Einstein was wrong

Quick Strange Quantum Facts

It appears:

- A “virtual particle” can appear and disappear, violating the law of the conservation of energy, impact other particles forever, and then disappear
- A particle can sometimes randomly jump a wall (or tunnel through it) even though it doesn’t have the energy, as defined by classical physics, to do so
- Observing/Measuring a quantum answer/particle changes it, forever more
- Viewing or measuring something, now, can appear to change what it did in the past
- Answers may be in another universe, with a trillion-trillion-trillion of us only different by one quantum answer (*Many World’s Theory*)
- Two most important to us in quantum computing are: **superposition** and **entanglement**

Quick Strange Quantum Facts

Superposition

- A quantum answer is always all possible answers
- A final, single measured answer is never guaranteed and cannot be predicted
- Example: Given the same inputs, coin may land heads, tails, or both heads and tails

Quick Strange Quantum Facts

<u>Fuzzy Entanglement</u>

- All quantum particles in nature will entangle with any other particle it meets, and most particles are meeting trillions of other particles every second
- When they entangle, the measured property of one entangled particle will always be the same answer on the other entangled particles
- Ex. If one spins right all the others spin right at the same time, no matter how far apart across the universe. Happens 6x the speed of light even though nothing can be faster than light
- They can no longer be considered separate systems…they are one system
- When computers are trying to get a single answer, they need to compute using a single particle to get a single answer (1 or 0), entanglement just complicates things, so quantum computer makers go to great lengths to not let particles meet other particles

“Those who are not shocked when they first come across quantum theory cannot possibly have understood it.”

Niels Bohr, Quantum Physicist and 1922 Nobel Prize Winner

“Any sufficiently advanced technology is indistinguishable from magic.”

Arthur C. Clarke, sci-fi author

What Is Quantum Computing?

What is Quantum Computing?

Traditional Computers

Traditional, classical, computers work using binary information

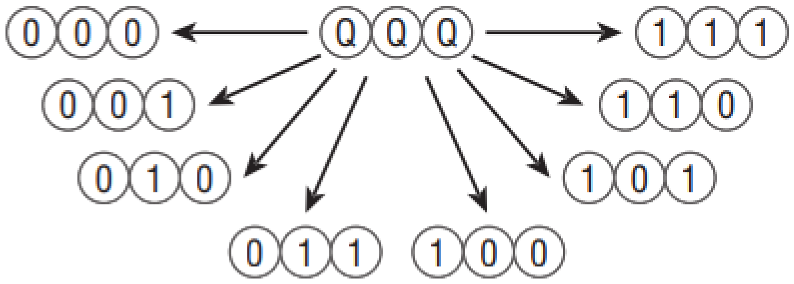
- Binary digit = bit
- Each bit can be 1 or 0, negative or positive charge, on or off
- Although each bit can one of two things, it can only be one thing at one time

1 bit = 1, 2 bits =2, 3 bits =3, etc.

What is Quantum Computing?

Quantum Computers

- First theorized in 1959 by Richard Feynman
- Quantum computers use quantum particles and properties to compute
- A quantum bit (or **qubit**) – can be used computationally as three states (0 or 1 or 0 and 1) AT THE SAME TIME (superposition while in cohered quantum states)
  - 1 qb=2-bits, 2 qb=4-bits, 3 qb=8-bits…at same time



- When read, becomes only a 0 or 1 forever more (decoherence)

What is Quantum Computing?

Quantum Computers

Qubits can be represented by any quantum attributes or property of any quantum particle (such as an electron or photon)

- Right spin, left spin (1 or 0)
- Up spin, down spin (1 or 0)
- +1 spin, -1 spin (1 or 0)
- Right polarization, left polarization (1 or 0)
- Color of wavelength
- Number of vibrations
- Etc.

What is Quantum Computing?

Quantum Computers

How to Make a Quantum Computer:

1. Pick the quantum particle and properties you want to represent 0's and 1's

   The qubits

2. Create/use physical quantum logic gates (AND, OR, NOT, etc.) that can represent and manipulate those 0's and 1's

   Ex. The polarization (direction) of photons and polarized filters that only allow photons of a certain polarization to pass

3. Run instructions/programs that manipulate those gates to solve problems
4. Measure the final state of the gates/registers when program finishes
5. Get a quantum answer

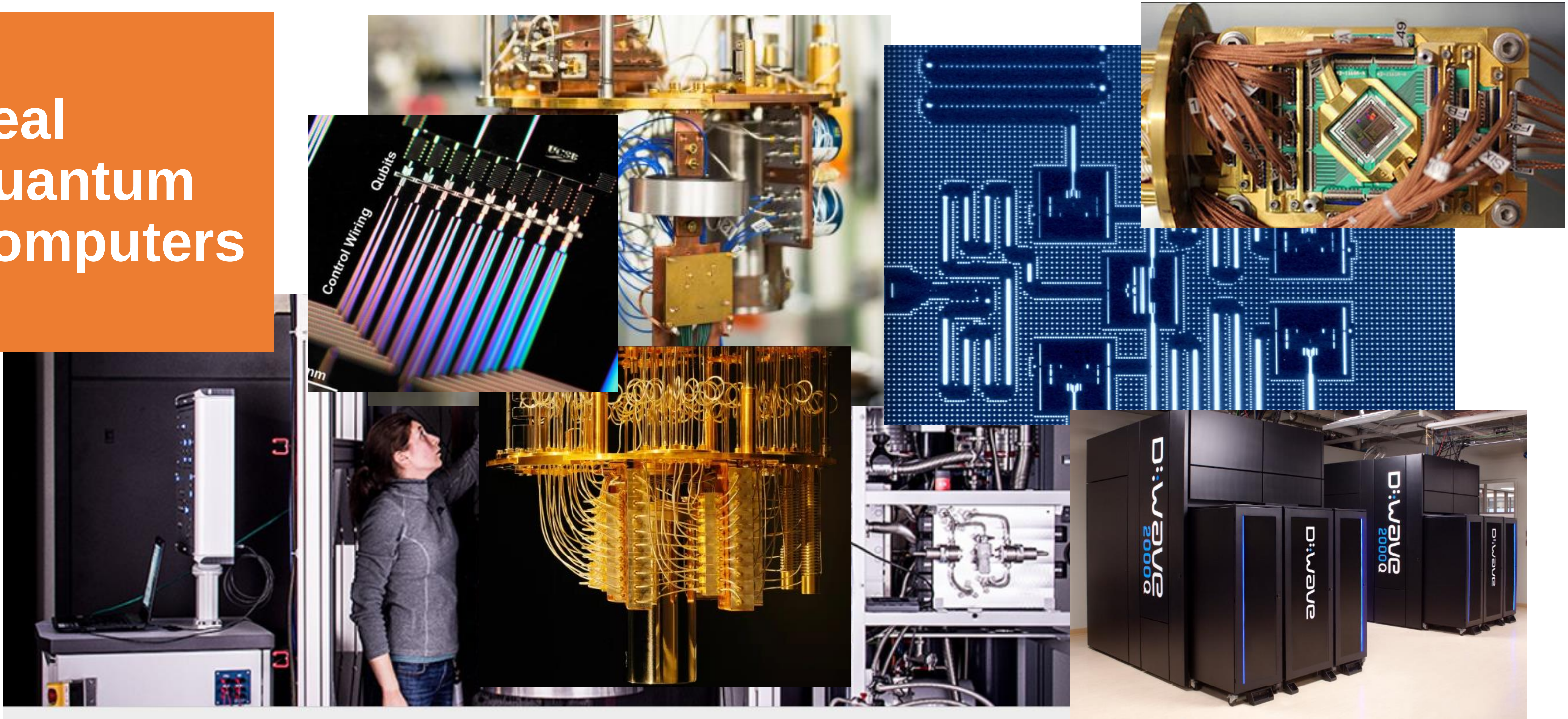
What is Quantum Computing?

Quantum Computers

- 1998 – First working quantum computer, 2-qubits
- 2000 – 5- and 7-qubit computers
- 2005 – 8-qubit computer
- 2006 – 12-qubit computer
- 2007 – 28-qubit computer
- 2012 – 84-qubit computer
- 2015 – 1000-qubit computer
- 2016 – Google develops quantum computer
- 2017 – 2048-qubit computer
- 2017 – IBM, Microsoft, announces quantum computers
- 2018 – Several quantum microprocessors available
- 2019 – Hundreds of early quantum computers available

What is Quantum Computing?

Real Quantum Computers



What is Quantum Computing?

Types of Quantum Computers

Not All Qubits Are Alike

- Many different types of quantum computers:
  - Superconducting (-460F temps)
  - Annealing
  - Trapped ion
  - Majorana fermion
    - Each method has advantages and disadvantages
- Right now, the quantum computers with the highest number of qubits, like 2000+, are called annealing, which aren't great at breaking crypto
- Universal gate quantum computers are better at breaking crypto, but so far have a smaller number of stable qubits
  - 72 qubits as of Sept. 2018
- Over hundreds of separate teams working on their own quantum computers

What is Quantum Computing?

Quantum Computers

<u>We Need More Stable Qubits</u>

- Stable qubits are very hard to make (right now)
  - Without the right conditions, they lose their needed quantum properties very quickly (decoherence = too much unwanted entangling)
  - Merely “observing” qubits makes them change
- Need them stable long enough (cohered) to complete a task and be able to observe outcome
- Most of today’s qubits need “error correcting” or “stabilization” or be “controllable” to work, which requires many more qubits than just the ones doing the work
- The number of stable, controllable qubits is increasing over time
  - But right now even those make a mistake once every 200 actions
- May need 1000 or a 1,000,000 error correcting qubits for every 1 stable qubit

What is Quantum Computing?

Quantum Computers

Today we have:

The richest nations, dozens of companies, spending tens of billions of dollars on quantum computing:

- Quantum computers
- Quantum microprocessors
- Cloud-connected quantum computers you can play with
- Quantum key distribution
- Quantum random number generators
- Quantum programming languages, development kits, compilers
- Quantum networking
- Quantum cryptography

What is Quantum Computing?

Quantum Computers

What Will Quantum Computers Give Us?

- New understanding of physics and our universe
- Solve complicated math quickly
- Give us incredible precision (military, weather, traffic mgmt.)
- New medicines, better solar cells, new chemicals
- True artificial intelligence
- Things we cannot imagine right now

What is Quantum Computing?

Quantum Computers

What Will Quantum Computers Give Us?

- Break most traditional public key crypto and every secret it protects
  - Any algorithm who's security relies on one of three hard mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem
  - Ex: RSA, DH, ECC, ElGamal, PKI, digital certificates, digital signatures, TLS, HTTPS, VPNs, HSMs, smartcards, WiFi protection, crypto-currencies, two-factor authentication which relies on digital certificates (e.g. FIDO keys, Google security keys, etc.), etc.
- New "unbreakable" encryption

What is Quantum Computing?

Traditional Computers

- If we were calculating all the possible combinations on a chessboard
  - 2^64
  - and each option was represented by a grain of rice
- Then the number of grains of rice would be as high as Mount Everest

X

=

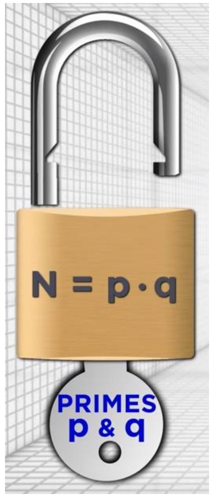
What is Quantum Computing?

Traditional Computers

- To brute force factor a 4096-bit prime number equation would take more than the known atoms in the universe
  - There are more than 125 million atoms in the period at the end of this sentence.
- Not enough energy in the known universe
- Conventional computers cannot factor equations/numbers this large
- Quantum computers can in seconds to minutes

How Does Quantum Break Public Key Crypto?

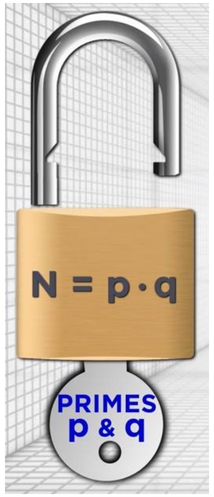
Quantum Break



- A **prime number** is any whole number after 1 that can only be divided by itself or one and get a whole number
  - 2,3,5,7,11,13,17,23,29,31, and so on
- Most traditional public key crypto (e.g. RSA, Diffie-Hellman, etc.) is based on the work effort needed to factor large prime number equations
  - **p * q = n**
    - p and q are prime numbers, n is a public key, can be very hard to figure out p and q
  - Simple Ex: What two prime numbers when multiplied together equal 15?
  - Answer: 3 x 5 = 15

How Does Quantum Break Public Key Crypto?

Quantum Break

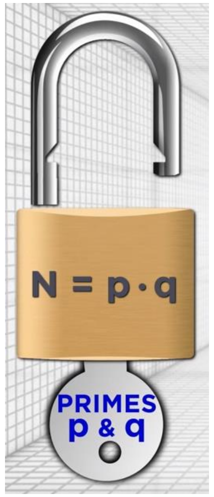


Another Simple Example

- p*q=187, what’s p and q?
- Answer: p and q = 17 and 11
- p*q= 84773093, what’s p and q?
- Answer: p and q = 9539 and 8887

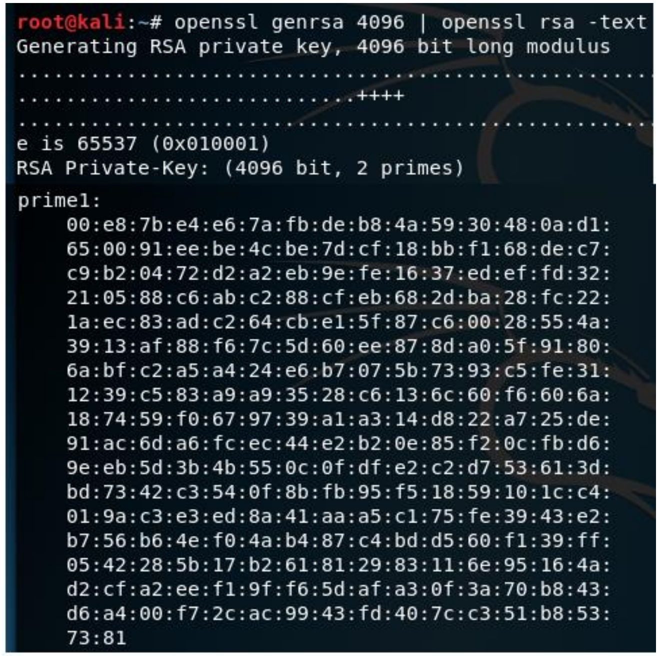
How Does Quantum Break Public Key Crypto?

Quantum Break



Another Simple Example

- Now assume N is a prime number 4096-bits/1234 decimal digits long

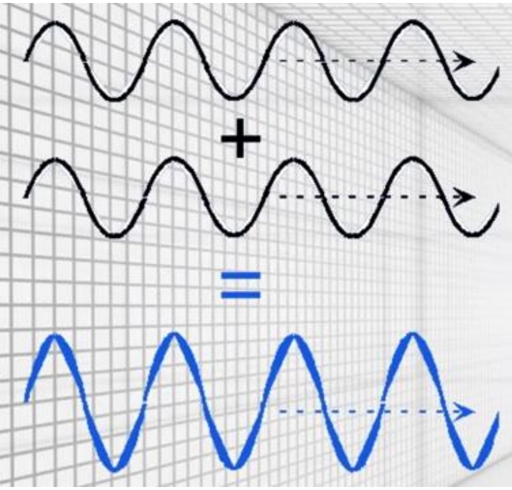


```
root@kali:~# openssl genrsa 4096 | openssl rsa -text
Generating RSA private key, 4096 bit long modulus
.....................................................
............................++++
.....................................................
e is 65537 (0x010001)
RSA Private-Key: (4096 bit, 2 primes)
prime1:
    00:e8:7b:e4:e6:7a:fb:de:b8:4a:59:30:48:0a:d1:
    65:00:91:ee:be:4c:be:7d:cf:18:bb:f1:68:de:c7:
    c9:b2:04:72:d2:a2:eb:9e:fe:16:37:ed:ef:fd:32:
    21:05:88:c6:ab:c2:88:cf:eb:68:2d:ba:28:fc:22:
    1a:ec:83:ad:c2:64:cb:e1:5f:87:c6:00:28:55:4a:
    39:13:af:88:f6:7c:5d:60:ee:87:8d:a0:5f:91:80:
    6a:bf:c2:a5:a4:24:e6:b7:07:5b:73:93:c5:fe:31:
    12:39:c5:83:a9:a9:35:28:c6:13:6c:60:f6:60:6a:
    18:74:59:f0:67:97:39:a1:a3:14:d8:22:a7:25:de:
    91:ac:6d:a6:fc:ec:44:e2:b2:0e:85:f2:0c:fb:d6:
    9e:eb:5d:3b:4b:55:0c:0f:df:e2:c2:d7:53:61:3d:
    bd:73:42:c3:54:0f:8b:fb:95:f5:18:59:10:1c:c4:
    01:9a:c3:e3:ed:8a:41:aa:a5:c1:75:fe:39:43:e2:
    b7:56:b6:4e:f0:4a:b4:87:c4:bd:d5:60:f1:39:ff:
    05:42:28:5b:17:b2:61:81:29:83:11:6e:95:16:4a:
    d2:cf:a2:ee:f1:9f:f6:5d:af:a3:0f:3a:70:b8:43:
    d6:a4:00:f7:2c:ac:99:43:fd:40:7c:c3:51:b8:53:
    73:81
```

- Traditional computers are not good at figuring out very large N’s
- Remember: Takes more guesses than all atoms in the known universe

How Does Quantum Break Public Key Crypto?

Quantum Break



How Quantum Computers Do It

Shor's Algorithm (1994)

- Cracks large prime equations very quickly if given (2 x qubits+1) as the key length you want to break
- "Due to the efficiency of the quantum Fourier transform, and modular exponentiation by repeated squarings."
- Start by creating all the possible answers for N=p*q all at once (superposition of states)
  - Take a wrong guess
  - Move from wrong guess to right answer in 8 quick steps
- Transform possible answers into sin waves and look for tallest

How Does Quantum Weaken Other Crypto?

Quantum Break

<u>How Quantum Computers Do It</u>

Grover's Algorithm (1996)

- Gives a quadratic speed up for certain types of "unordered searches"
- Applies to cracking symmetric encryption keys, hashes, and random number generators
- Halves the protection of those key sizes
- Ex. SHA-256 becomes SHA-128, AES-256 becomes AES-128, etc.

How Long Till Quantum Computing Breaks Public Key Cryptography?

When Will Quantum Break Public Key Crypto?

Quantum Break

Bottom Line

- Many quantum physicists think we’ll have enough stable qubits within a few years (if it’s not already done) to break public crypto which uses the large prime factoring work effort for protection
- But who really knows??

When Will Quantum Break Public Key Crypto?

Quantum Break

<u>Bottom Line</u>

In 2016, NIST/NSA, “NOW” is the time to prepare

Commercial National Security Algorithm Suite and Quantum Computing FAQ

Q: Why is now the right time to make an announcement?

A: Choosing the right time to champion the development of quantum resistant standards is based on 3 points: forecasts on the future development of a large quantum computer, maturity of quantum resistant algorithms, and an analysis of costs and benefits to NSS owners and stakeholders. NSA believes the time is now right—consistent advances in quantum computing are being made, there are many more proposals for potentially useful quantum resistant

https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf

How You Can Prepare for the Quantum Break

Preparing for Quantum Break

Scenarios

What do the different possible break scenarios look like?

Preparing for Quantum Break

Timing

Break Scenarios

- It’s already happened but we don’t know about
- It’s going to happen in the next few years
- It’s going to happen after the next few years
- It’s never going to happen

I would not put my money on the last one.

Preparing for Quantum Break

Who? Cost?

Break Scenarios

- Stays in the realm of nation-states for a long-time
- Gets picked up by monied groups and competitors
- Available in cloud form for cheap
- Past crypto breaks went from the realm of millions of dollars to accomplish to tens of thousands of dollars in just a few years
- Interested parties are likely storing encrypted communications for future breaks already

Preparing for Quantum Break

Will We Be Prepared?

Break Scenarios

- If we are lucky, the quantum break prep proceeds like the global SHA1 to SHA2 migration (slower than we liked, but orderly, and ahead of the worst problems)
- Might happen faster than companies and vendors are prepared
  - NSA said to move to post-quantum in Jan. 2016, what have you or any of your vendors or partners done?
- Likely to be a mix of prepared and not prepared when time comes

Preparing for Quantum Break

Prepare

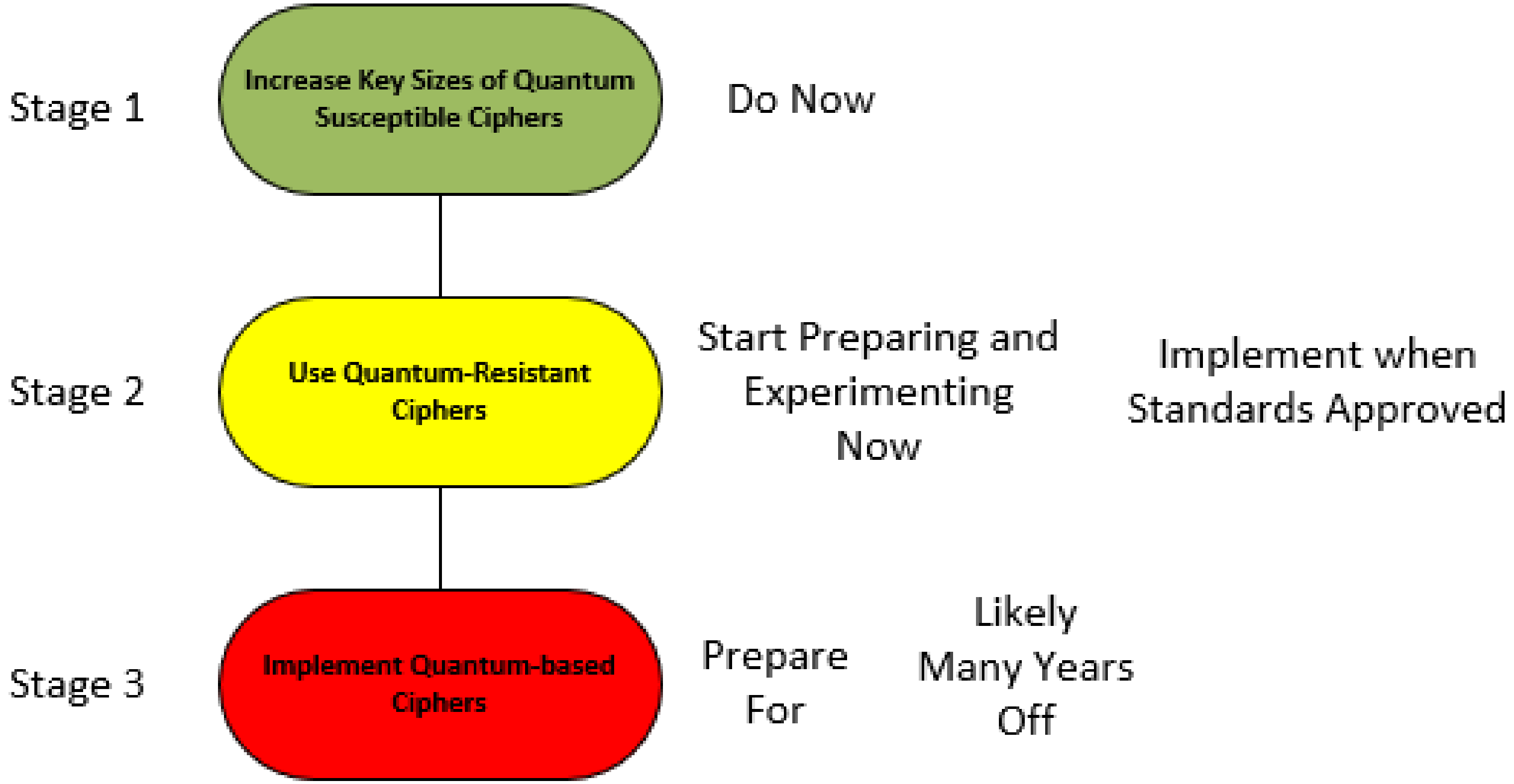
Preparing

- **Education** (this slide deck and keeping up on advances)
  - Your company, your vendors, your third parties
- **Take a data protection inventory** – what secrets really need to be protected, and for how long? Which are at risk from quantum break?
- **Use/Be moving toward quantum-resistant crypto**, where and when possible
- **Pressure your vendors over quantum break preparation**
- At least demand **“crypto-agility”**
- **Prevent eavesdropping today on very high-value data**

Preparing for Quantum Break

Prepare

Post-Quantum Protection Plan



Preparing for Quantum Break

Prepare

<u>Post-Quantum Protection Plan</u>

Immediate

- Make sure your symmetric key and hash sizes are 256-bits or bigger
- Move asymmetric key sizes to 4096 (optional)
- Protect critical secrets from eavesdropping

Soon

- Move to quantum-resistant asymmetric ciphers when possible

Later

- Move to quantum ciphers

Preparing for Quantum Break

Prepare

Post-Quantum Protections

Symmetric encryption is not as vulnerable

- 128-bit is bare minimum (weakly quantum-resistant)
- 192-bit is better, 256-bit even better, 512-bit very resistant

- **AES** is still good
- **Blowfish, Twofish**
- **Serpent, Chacha/Salsa20**
- **SNOW 3G**

Unfortunately, traditional public key crypto is used to protect the transmission of plaintext symmetric keys most of the time

Preparing for Quantum Break

Prepare

Post-Quantum Protections

Quantum-Resistant Hashes (when using 256-bit and larger sizes)

- **SHA2/SHA3**
- **SHAKE**
- **PBKDF2**
- **RIPEMD**
- **ARGON2**
- **Blake2**

Preparing for Quantum Break

Prepare

NIST Quantum-Resistant Cipher and Digital Signatures

- **Lattice-based**
- **Multivariate-based**
- **Code-based**
- **Hash-based**
- **Zero Knowledge Proof**
- **Isogeny-based**

Asymmetric Encryption/KEMs	Type	Signatures	Type
CRYSTAL-Kyber	Lattice	CRYSTALS-Dilithium	Lattice
FrodoKEM	Lattice	FALCON	Lattice
LAC	Lattice	qTESLA	Lattice
NewHope	Lattice	SPHINCS+	Hash
Three Bears	Lattice	GeMSS	Multivariate
NTRU	Lattice	LUOV	Multivariate
NTRU Prime	Lattice	MQDSS	Multivariate
SABER	Lattice	Rainbow	Multivariate
Round5	Lattice	Picnic	Zero Knowledge Proof
Classic McEliece	Code		
NTS-KEM	Code		
BIKE	Code		
HQC	Code		
LEDAcrypt	Code		
Rollo	Code		
RQC	Code		
SIKE	Isogeny		

- See https://en.wikipedia.org/wiki/Post-quantum_cryptography

Unfortunately, almost none are generally available yet

Preparing for Quantum Break

Prepare

NIST Quantum-Resistant Cipher and Digital Signatures -3rd Round Candidates

- 3rd round candidates announced in July 2020

Third Round Finalists

Public-Key Encryption/KEMs
Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

Digital Signatures
CRYSTALS-DILITHIUM
FALCON
Rainbow

Alternate Candidates

Public Key Encryption/KEMs
BIKE
FrodoKEM
HQC
NTRU Prime
SIKE

Digital Signatures
GeMSS
Picnic
SPHINCS+

Preparing for Quantum Break

Prepare

Post-Quantum Protections

Use quantum-based ciphers and components, including

- Quantum Random Number Generator
  - Verifiably and guaranteed random
  - Many existing ones
  - Online one at https://qrng.anu.edu.au/
- Quantum Key Distribution (QKD)
- Use Post-Quantum Cryptography
- Quantum Encryption
  - Perfectly secure in theory
  - If anyone observes the data, you'll know

Preparing for Quantum Break

Prepare

Post-Quantum Protections

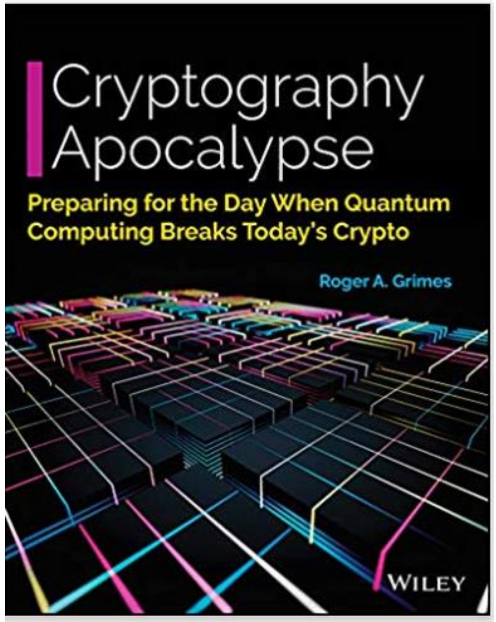
Open Quantum Safe Project (https://openquantumsafe.org/)

- Group dedicated to helping to implement post-quantum crypto
- Open source C-library (**liboqs**) to implement some post-quantum ciphers
- API
- Testing and benchmarking
- Forked quantum-resistant versions of OpenSSL and OpenSSH

More Learning

Info

- **https://www.amazon.com/Cryptography-Apocalypse-Preparing-Quantum-Computing/dp/1119618193**
  - Appendix at end of book lists dozens of sources
- https://en.wikipedia.org/wiki/Quantum_computing
- Go to Youtube and Amazon and search on "quantum"



My free primers:

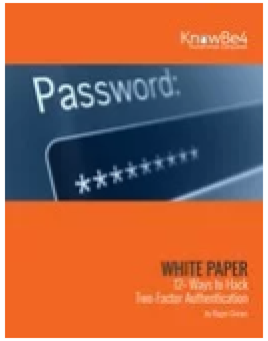
- https://www.linkedin.com/pulse/quantum-mechanics-computing-primer-roger-grimes/
- https://www.linkedin.com/pulse/quantum-supremacy-achieved-what-means-you-your-company-roger-grimes/

Resources

Free IT Security Tools

- Domain Doppelgänger
- Awareness Program Builder
- Domain Spoof Tool
- Mailserver Security Assessment
- Phish Alert
- Ransomware Simulator
- Weak Password Test
- Phishing Security Test
- Second Chance
- Email Exposure Check Pro
- Training Preview
- Breached Password Test

Whitepapers



12+ Ways to Hack Two-Factor

All multi-factor authentication (MFA) mechanisms can
know how to defend against MFA hacks? This whitepa
those attacks.

Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

CEO Fraud Prevention Manual

CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.

» Learn More at www.KnowBe4.com/Resources «

Thank You!

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/