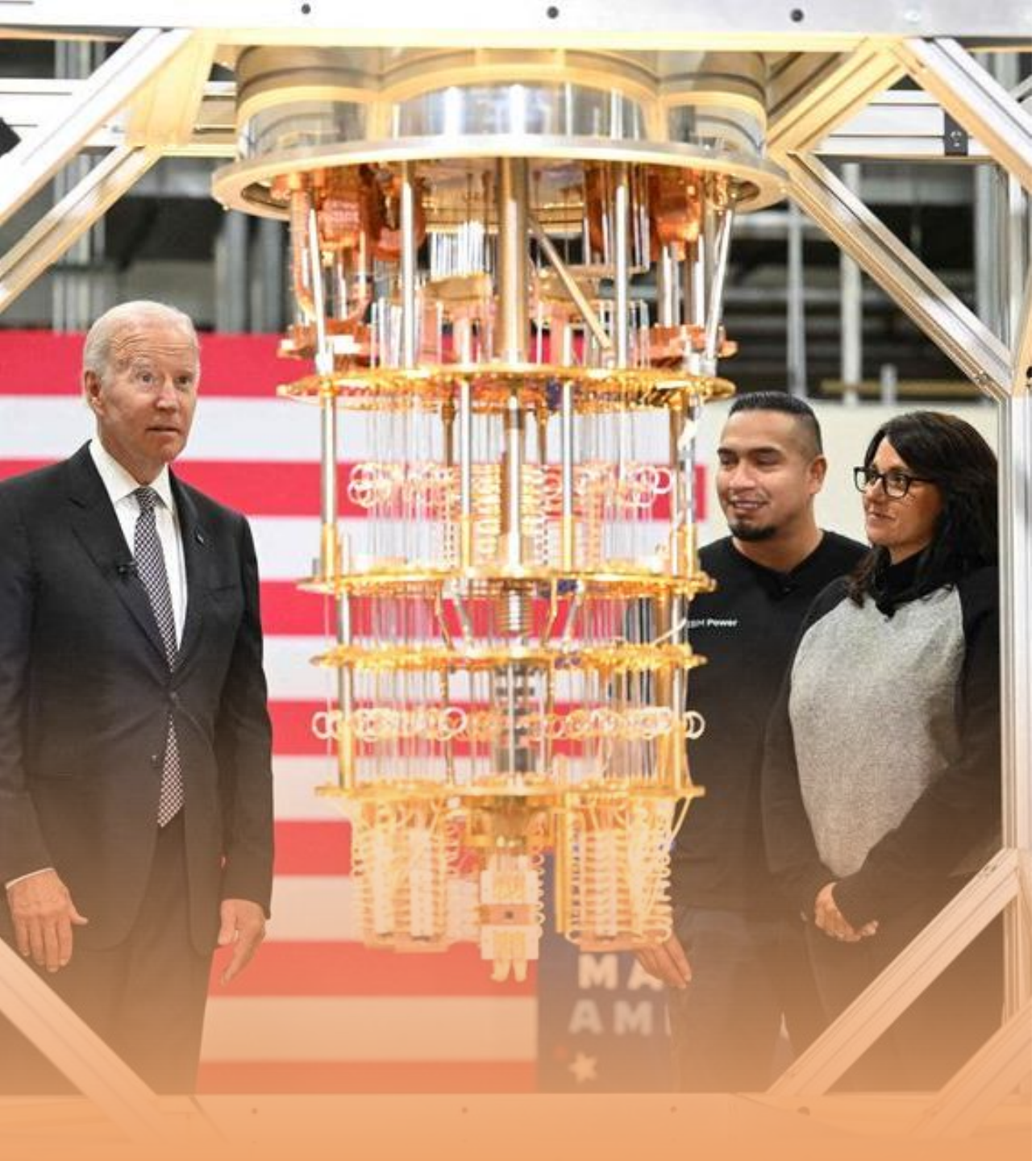
POST-QUANTUM CRYPTOGRAPHY (PQC)

The Next Y2K?

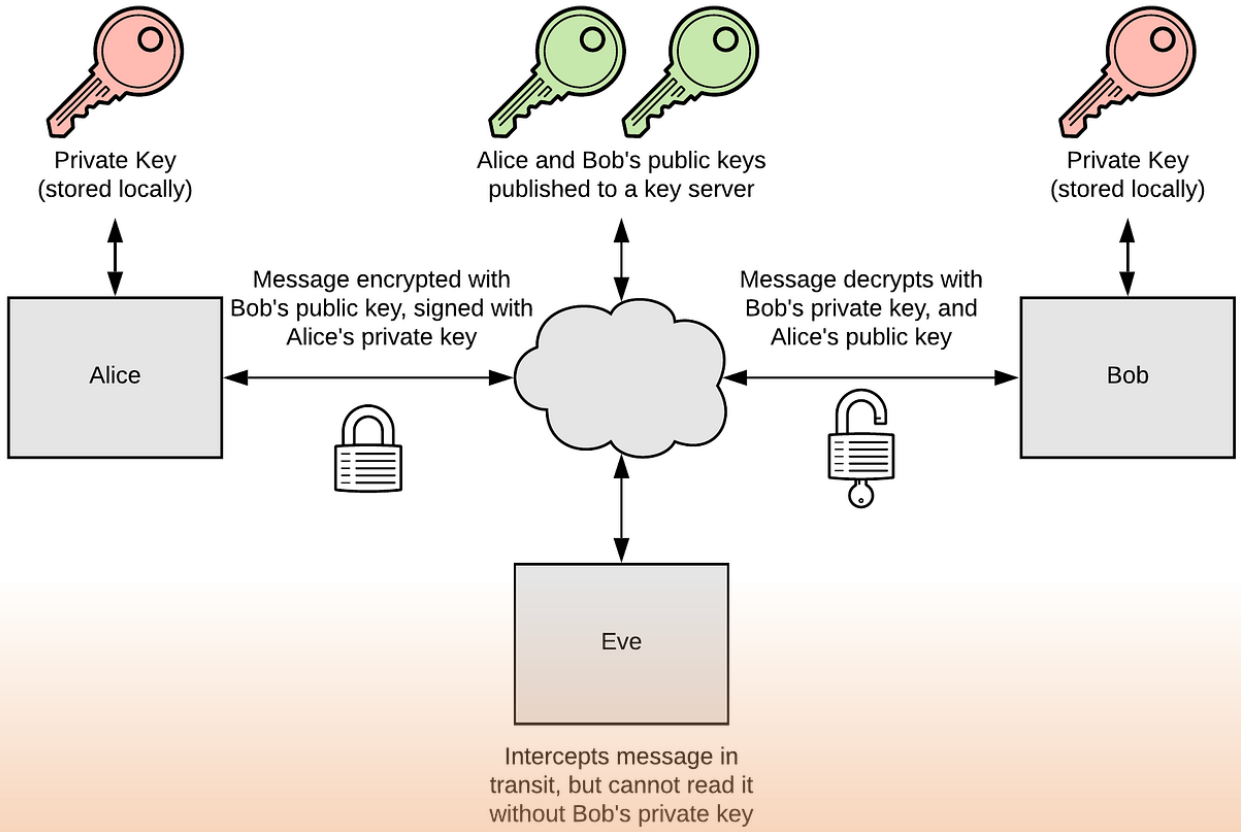


QUANTUM COMPUTERS

- Supercooled, awesome things that use quantum mechanics to solve mathematical problems faster than regular computers
- Not faster at all kinds of math
- Brilliantly fast at finding prime factors of extremely large numbers

OH SNAP

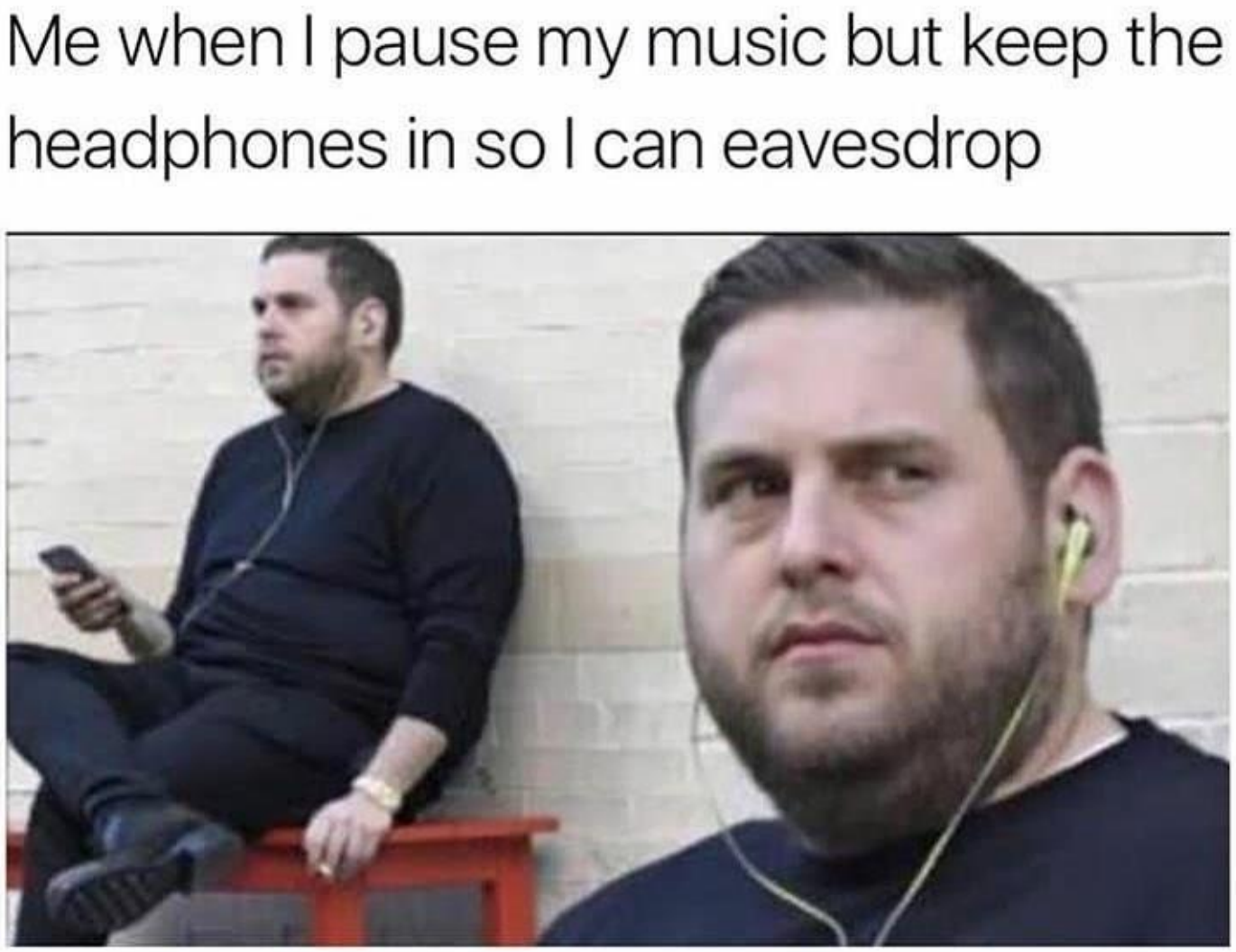
- HTTPS rides on keys made from big numbers made from big primes
- Regular computers take billions of years to solve that math
- Quantum computers take a short while
- Once decoded, all encrypted traffic is easily read



ATTACK #1: HARVEST NOW, DECRYPT LATER

ATTACK #2:
REAL TIME DECRYPT

- Quantum computer breaks, regular PC uses key to eavesdrop
- Passive listeners hard to detect
- Communicating parties unaware until captured data revealed to them in public or private OR
- Evidence that communications channels are compromised comes to light

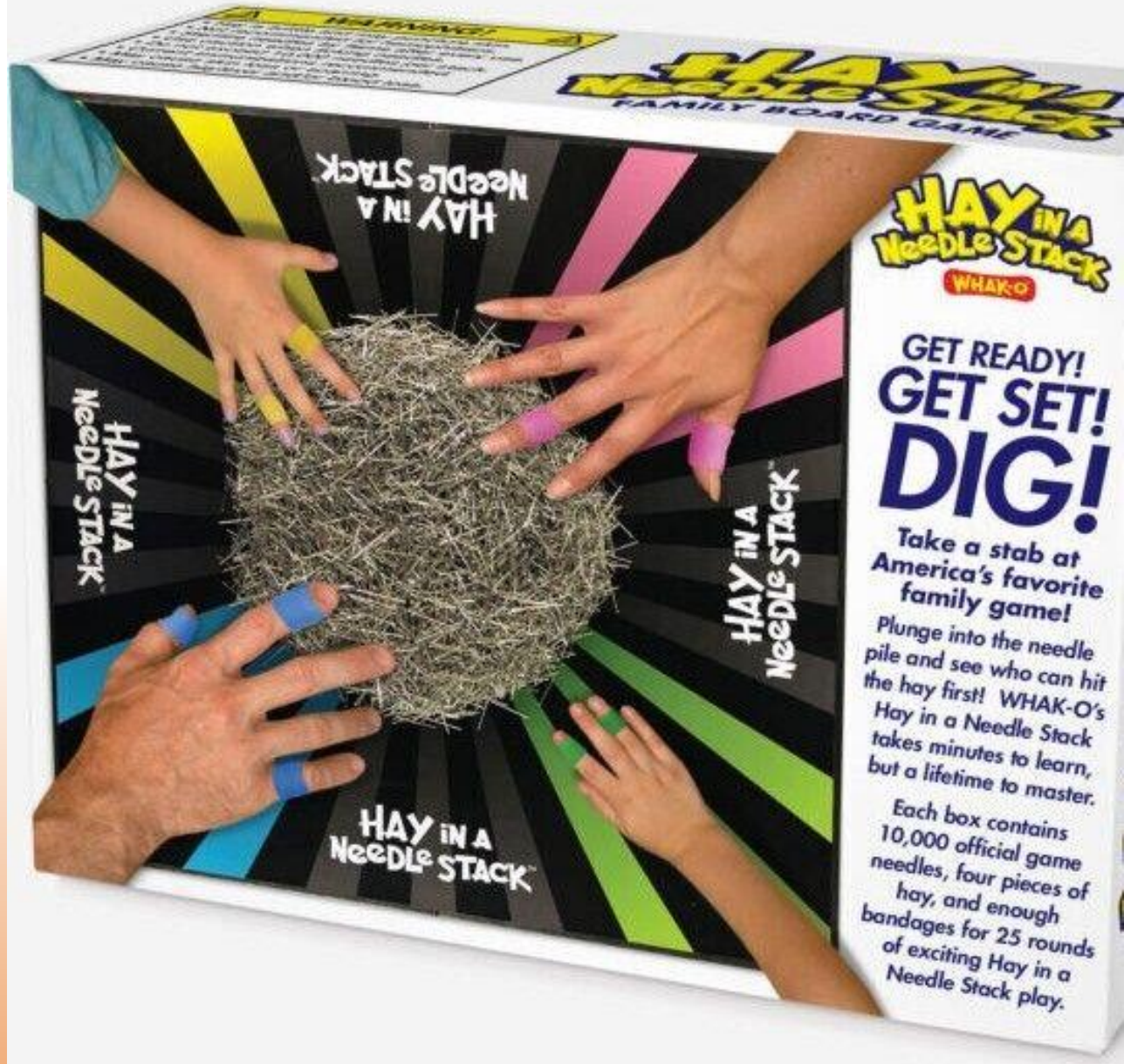


WHEN DO WE FACE QUANTUM?

- Estimates vary on “commercially-ready” quantum computer
- 5-25 years or so – think Y2K, but with no date where we know it’s a thing
- “Espionage-ready” quantum computing will be ready prior to commercially-ready

PQC PROBLEM: PART ONE

- We have to first find where we are using cryptography.
- Crypto-visibility can be attained three ways:
- Network packet analysis
- Application analysis
- Desktop agent



PQC PROBLEM: PART TWO
REPLACING CRYPTO IN APPS MAY BE DIFFICULT

PQC PROBLEM: PART THREE

- Will PQC algorithms be usable by current regular PCs?
- Those using lattice mathematics look most promising
- Overhead remains a concern, especially in real-time trading applications

PQC PROBLEM: PART FOUR

- Are the PQC encryptions safe from traditional hacking?
- Do we have legacy gear that won't support PQC encryption suites?
- Will all vendors keep their applications PQC-safe?
- How do we keep safe with encryption as ***all*** computers get faster?

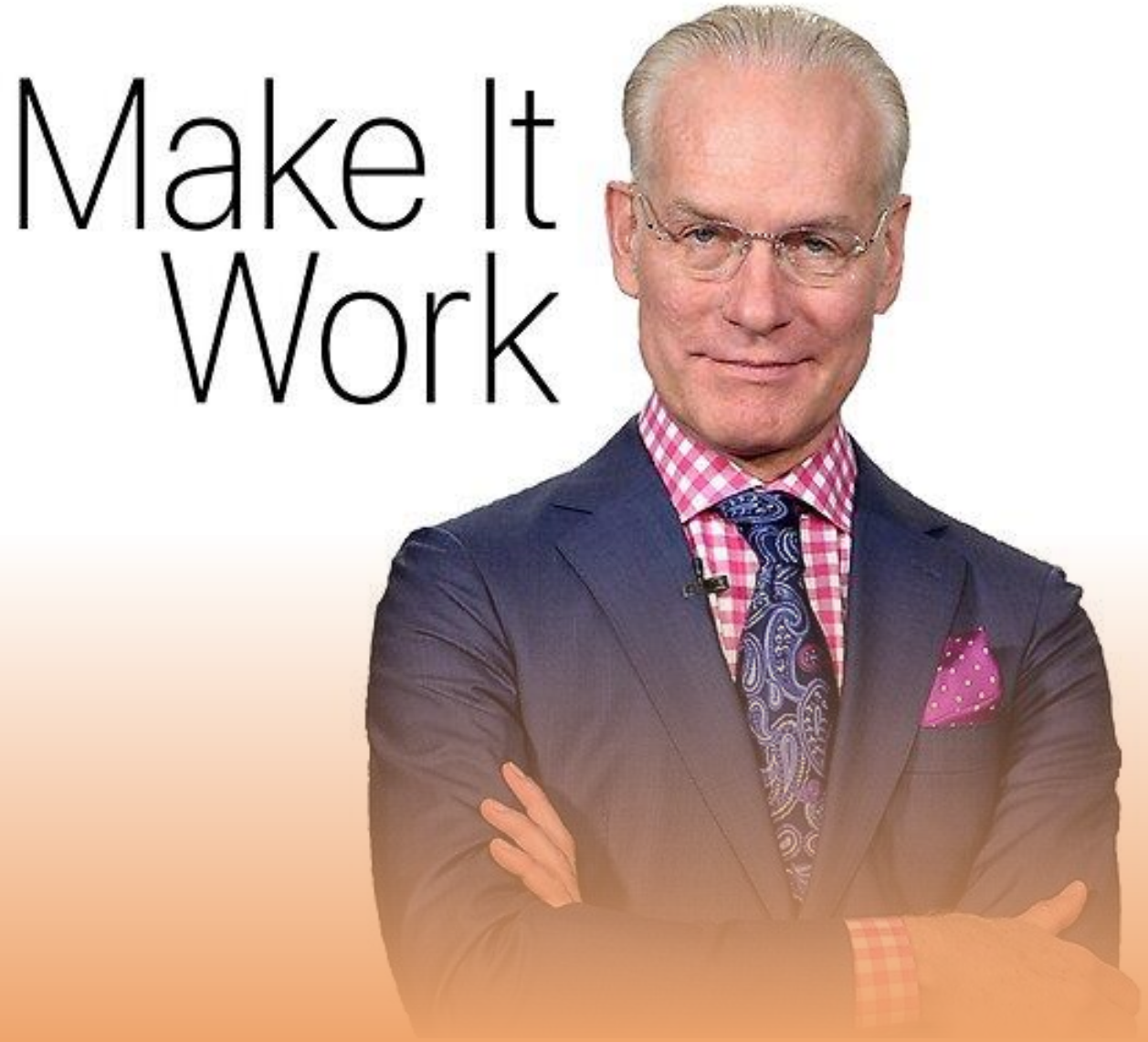
GOOD NEWS: WE DO HAVE SOLUTIONS

Disclaimer: I am a partner with the one I think is best

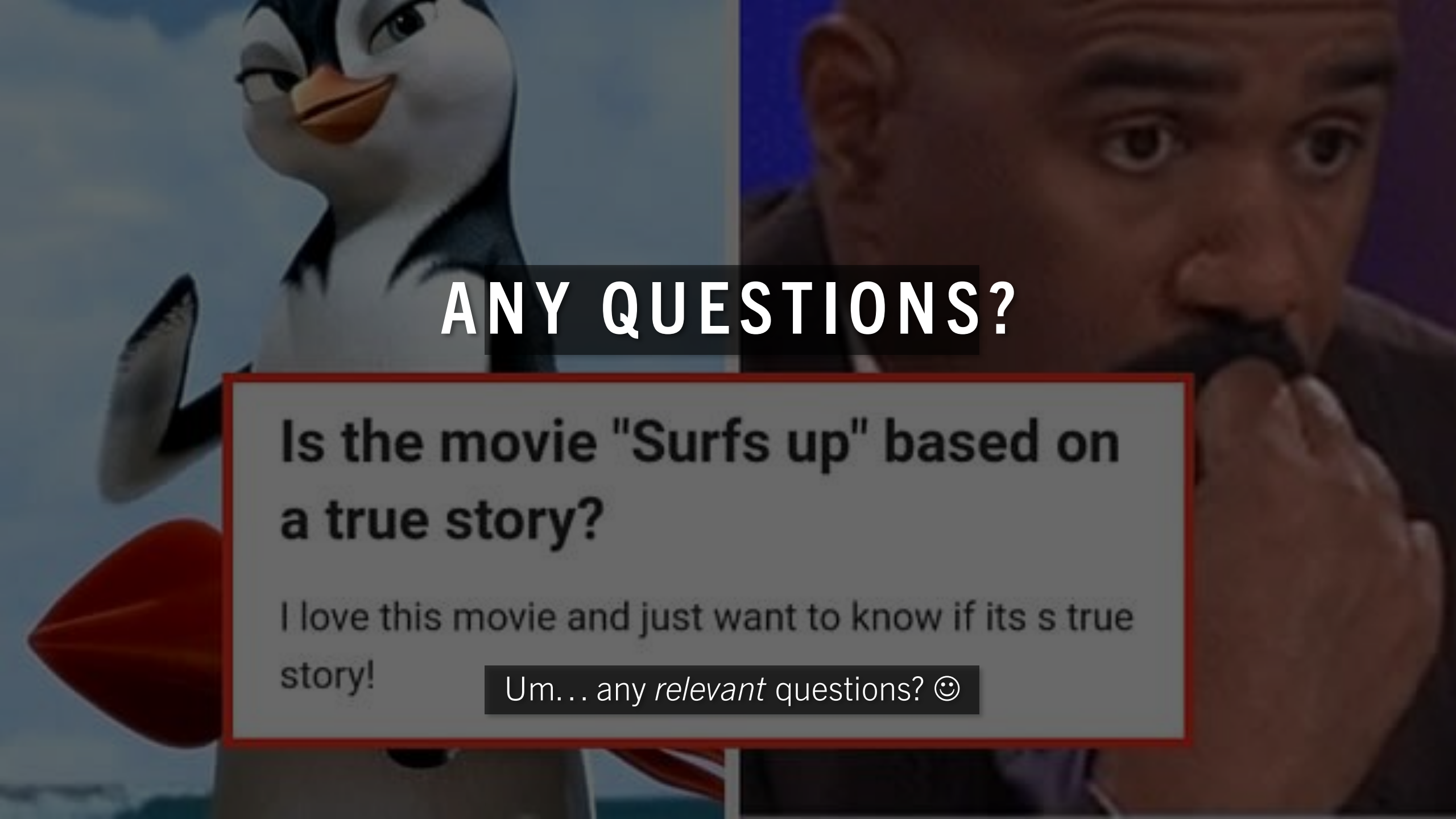
☺

HOW TO MAKE IT ALL WORK, END-TO-END

- Visibility: network tap, application probing, desktop agent – deploy and scrutinize
- Prioritize: Replace currently vulnerable, prioritize asymmetric, symmetric is good to go
- Replacement: Use central crypto repository, where applications check out and use latest suites
- Repository: Once we have PQC algorithms that are CISA tested and approved, add them in
- Wrapper: for applications that can't or won't upgrade, require that their traffic passes through PQC-ready gateway



- “Sell me this pen.”
- WRONG: “This is the best pen, ever”
- RIGHT: “Sure thing. Send me a quote request for how many you need, but be sure that it’s been encrypted with PQC-ready crypto suites.” ☺
- Demonstrating the need for PQC preparation and tools is job one where you work
- Once demonstrated, start assessing vendors and get to work as soon as budgetarily possible.
- 5-25 years could suddenly become 2-4 years with breakthroughs
- If you remember Y2K, remember that we beat it only because we worked hard before the deadline


ANY QUESTIONS?
Is the movie "Surfs up" based on a true story?
I love this movie and just want to know if its s true story!
Um... any *relevant* questions? ☺

OBLIGATORY FINAL SLIDE

Thank you for your time!