Cryptography and Network Security

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

(1) Public-Key Cryptography

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

PK Cryptography

Using math and computational difficulty

for: confidentiality

& authentication

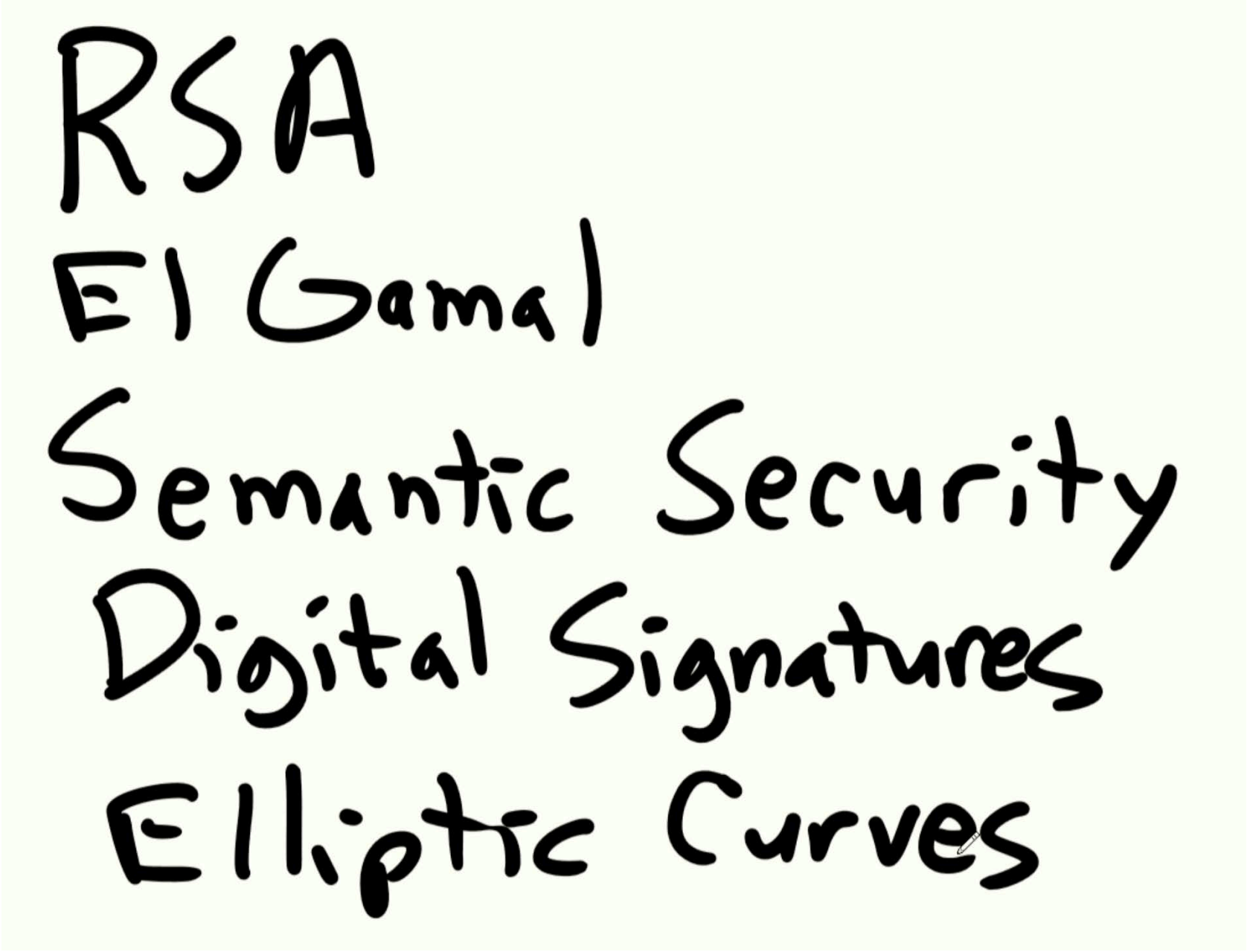
Context

Invention

Number Theory

Computational Complexity

Key Establishment



Homomorphic Properties Attacks & Security Looking Ahead

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(2) PK Cryptography: Context

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

"Keyless" Crypto

hash functions: file → "digest"

should be:

collision resistant

no h(file1) = h(file2)

CR

one-way

can't find file from h(file)

OW

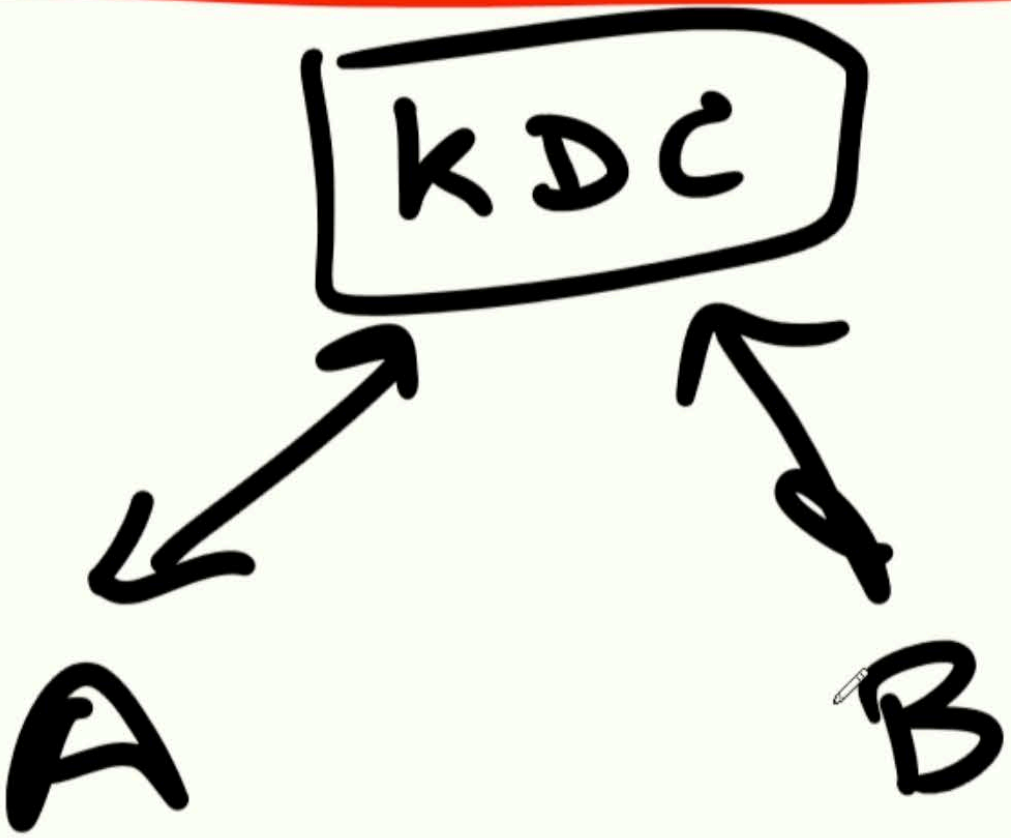
Symmetric crypto

Same key used by Alice & Bob

block ciphers (DES, AES)

message authentication codes (HMAC)

Key Distribution Centers



THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(3) PK Cryptography: Invention

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

Invention of PK Crypto

Diffie & Hellman "New Directions in Cryptography"

Merkle "Secure Communications over an Insecure Channel"

Different keys used by Alice & Bob

$$PK, Sk \leftarrow \text{keygen}$$

$$C \leftarrow E(PK, M)$$

C: ciphertext; M: plaintext

$$M \leftarrow D(sk, C)$$

Also digital signatures

$sig \leftarrow Sign(SK, M)$

$Verify(PK, M, sig)$

$\rightarrow$ True/False

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(4) PK Cryptography: Number Theory

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

Modular Math

$$3^2 + 7 = 5 \pmod{11}$$

Powering Up (Repeated Squaring)

$$3^{101} \pmod{197} = 3 \cdot 3^{100} \pmod{197}$$

$$3^{100} \pmod{197} = (3^{50})^2 \pmod{197}$$

Primes

2, 3, 5, 7, 11, ...

To find a large prime:

Pick a large random integer p

accept p as prime if

$$3^{p-1} = 1 \pmod{p}$$

else restart

Generators

For every prime p there is a "generator" g such that

$$g^0, g^1, \ldots, g^{p-2}$$

give all nonzero mod p

Easy to find p & associated generator g

Example: mod p p=5 g=3

$3^0 = 1$

$3^1 = 3$

$3^2 = 4$

$3^3 = 2$

$3^4 = 1$

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(5) PK Cryptography: Computational Complexity

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

Computational Complexity

Most crypto is based on assumptions

Examples:

$P \neq NP$

hash fn is CR or OW

Factoring

Given product $n = p \cdot q$
of two large primes p, q
it is (assumed) hard to find p, q

Stanley Jevons Challenge (1874)

$8616460799 = ?$
$89681 \cdot 96079$

Discrete Logarithm

Given p, g & $y = g^x \bmod p$

it is infeasible to find x

Example:

$14 = 3^x \pmod{31}$ what is x?

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(6) PK Cryptography: Key establishment

Ronald L. Rivest

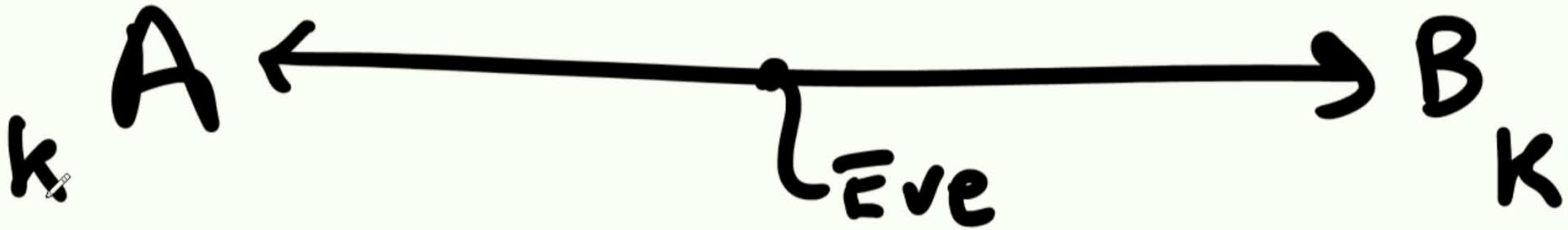
Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

Diffie-Hellman Key Establishment

How can Alice & Bob establish a secure shared secret key over an insecure channel?



Method: prime p, generator g

$A \rightarrow B$: $g^a \bmod p$ (a secret to A)

$B \rightarrow A$: $g^b \bmod p$ (b secret to B)

$K = (g^a)^b = (g^b)^a = g^{ab} \bmod p$

Eve can't compute g^{ab} from g^a & g

Hybrid Encryption (TLS)

setup session key K using DH

use AES to encrypt msgs thereafter

Forward secrecy property:

once A & B erase K, a, b, M

Eve gains nothing by hacking into their laptops

a, b, K are "ephemeral" keys

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(7) PK Cryptography: RSA

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

RSA (Rivest-Shamir-Adleman, 1977)

Based on difficulty of factoring

Setup:

$e = 3$ or $2^{16}+1$

p, q large random primes
($p-1, q-1$ not multiples of e)

$PK = (n, e)$ where $n = p \cdot q$

$SK = (n, d)$

where $d = e^{-1} \pmod{(p-1)\cdot(q-1)}$

To encrypt M with $PK(n,e)$:

$$C = M^e \pmod{n}$$

To decrypt C with $SK(n,d)$:

$$M = C^d \pmod{n}$$

Example: $p=5, q=11 \quad n=55$

$e=3, d=27$

Encrypt $m=7$

$$C = 7^3 \pmod{55} = 13$$

Decrypt $c=13$

$$m = 13^{27} \pmod{55} = 7$$

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(8) PK Cryptography: El Gamal

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

El Gamal PK Cryptosystem (1985)

Based on discrete log problem

large prime p, generator g

SK x random in $0, 1, \ldots, p-2$

PK $y = g^x \pmod{p}$

To encrypt m:

pick r random in $0, 1, \ldots, p-2$

$$c = (a, b) = (g^r, m \cdot y^r)$$

To decrypt $c = (a, b)$

$$m = b / a^x \pmod{p}$$

Example:

$p = 5, g = 3, x = 2, y = 3^2 = 4$

$m = 2, r = 3$

$c = (a, b) = (3^3, 2 \cdot 4^3)$

$= (2, 3)$

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(9) PK Cryptography: Semantic Security

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

Semantic Security

= indistinguishability under chosen plaintext attack IND-CPA

Goldwasser-Micali: 1982

Adv can't distinguish

E(a) from E(b)

even if he knows (or picks) a & b.

E("dog") or E("cat")

?

requires randomized encryption

El Gamal semantically secure

assuming DDH (Decision Diffie Hellman)

given g^x, g^r, and g^s

Adv can't tell if $g^s = g^{xr} \pmod p$

or not

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(10) PK Cryptography: Digital Signatures and Certs

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

Digital signatures:

SK used to sign M (or hash of M):

$Sig = Sign(SK, M)$

M, sig → recipient

PK used to verify

$Verify(PK, M, sig) = True/False$

Security

Adv can't forge signatures on new messages, even after seeing many valid signatures on messages of his choice!

Certificates

A certificate is a signed statement that a PK belongs to a named party.

Example: Verisign says (and signs) stmt that "Google's Pk is $n = \ldots, e = \ldots$"

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(11) PK Cryptography: Elliptic Curves

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

PROFESSIONAL EDUCATION

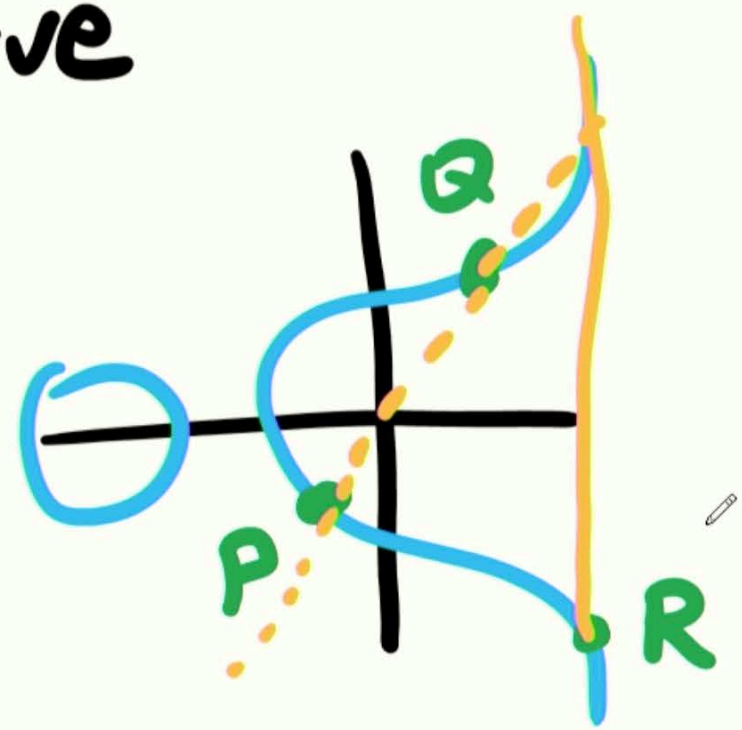
CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

Elliptic Curves

Replaces "mod p" or "mod n" with operations over elliptic curve

$$(x,y): y^2 = x^3 + ax + b$$

$$P + Q = R$$



Advantages:

- more compact
- often faster
- admits new functionalities via "pairing functions"

$$e(g^a, g^b) = e(g,g)^{ab}$$

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(12) PK Cryptography: Homomorphic Properties

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

Homomorphic Properties

operation on ciphertext ≡
operation' on plaintext

Example: $E(a+b) = E(a) \cdot E(b)$

Fully Homomorphic Encryption (FHE):
Can do for a "complete" set of operations

Voting Application

Each voter submits $E(v)$

$v=1$ for "for" & $v=0$ for "against"

$$E(v_1) \cdot E(v_2) \cdot \dots \cdot E(v_n)$$

$$= E(v_1 + v_2 + \dots + v_n)$$

decrypt

$$v_1 + v_2 + \dots + v_n$$

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(13) PK Cryptography: Attacks and Security

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

What can Adversary do?

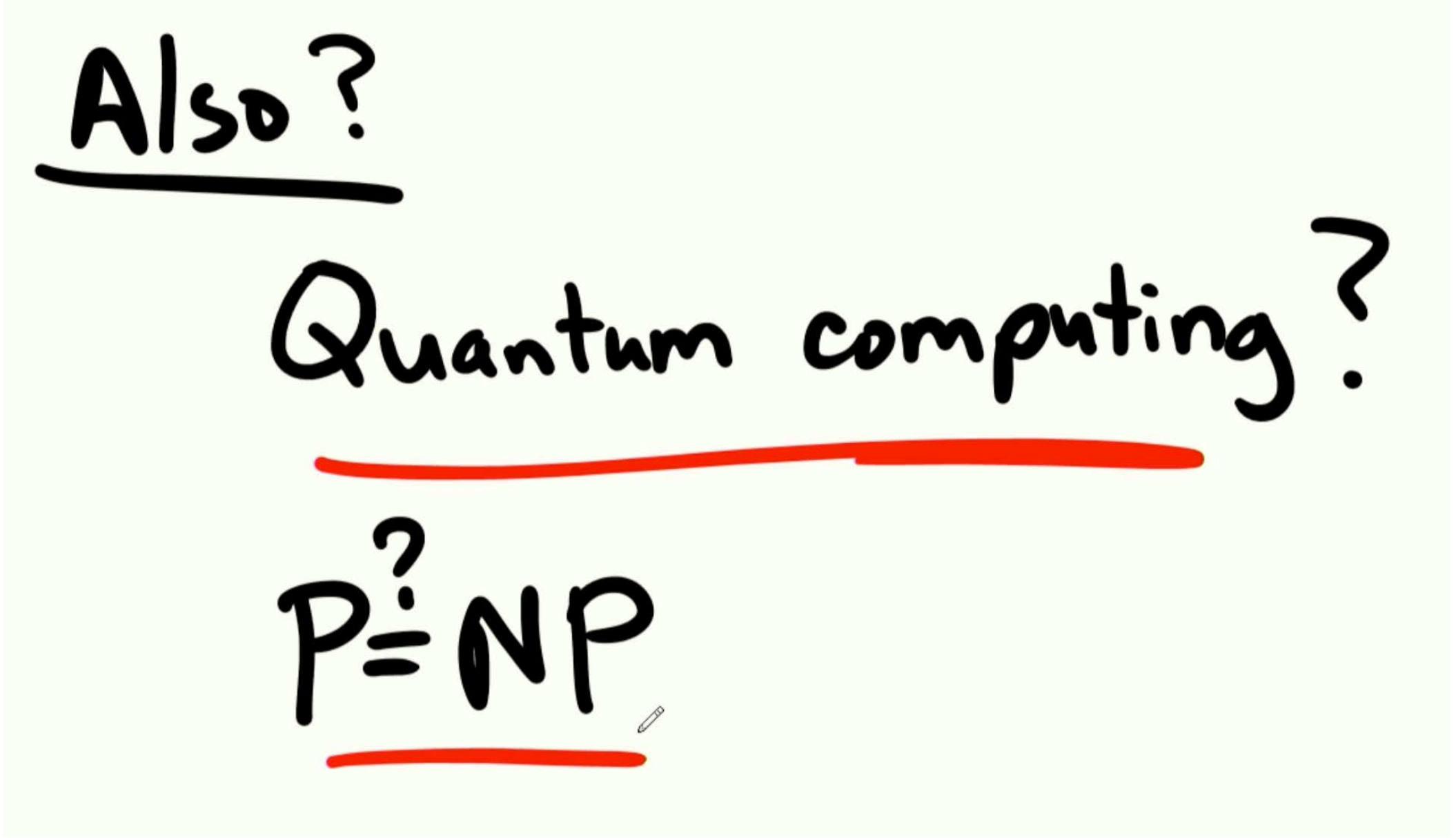
- Steal keys (malware)
- using PK
- get decryptions of chosen ciphertexts (IND-CCA)
- exploit implementation
- bugger implementation
- exploit protocol

Factoring (DL Similar)

768-bit # factored

1024-bit # - maybe in a few years

2048-bit # - many decades, if ever



THANK YOU

Ronald L. Rivest

Vannevar Bush Professor

(14) PK Cryptography: Looking Ahead

Ronald L. Rivest

Vannevar Bush Professor

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

Shafi Goldwasser:
MPC, Secret Sharing, Distributed Trust

Vinod Vaikuntanathan: Homomorphic & Functional Encryption

Dave Clark: Network Security & Protocol Design

THANK YOU

Ronald L. Rivest

Vannevar Bush Professor