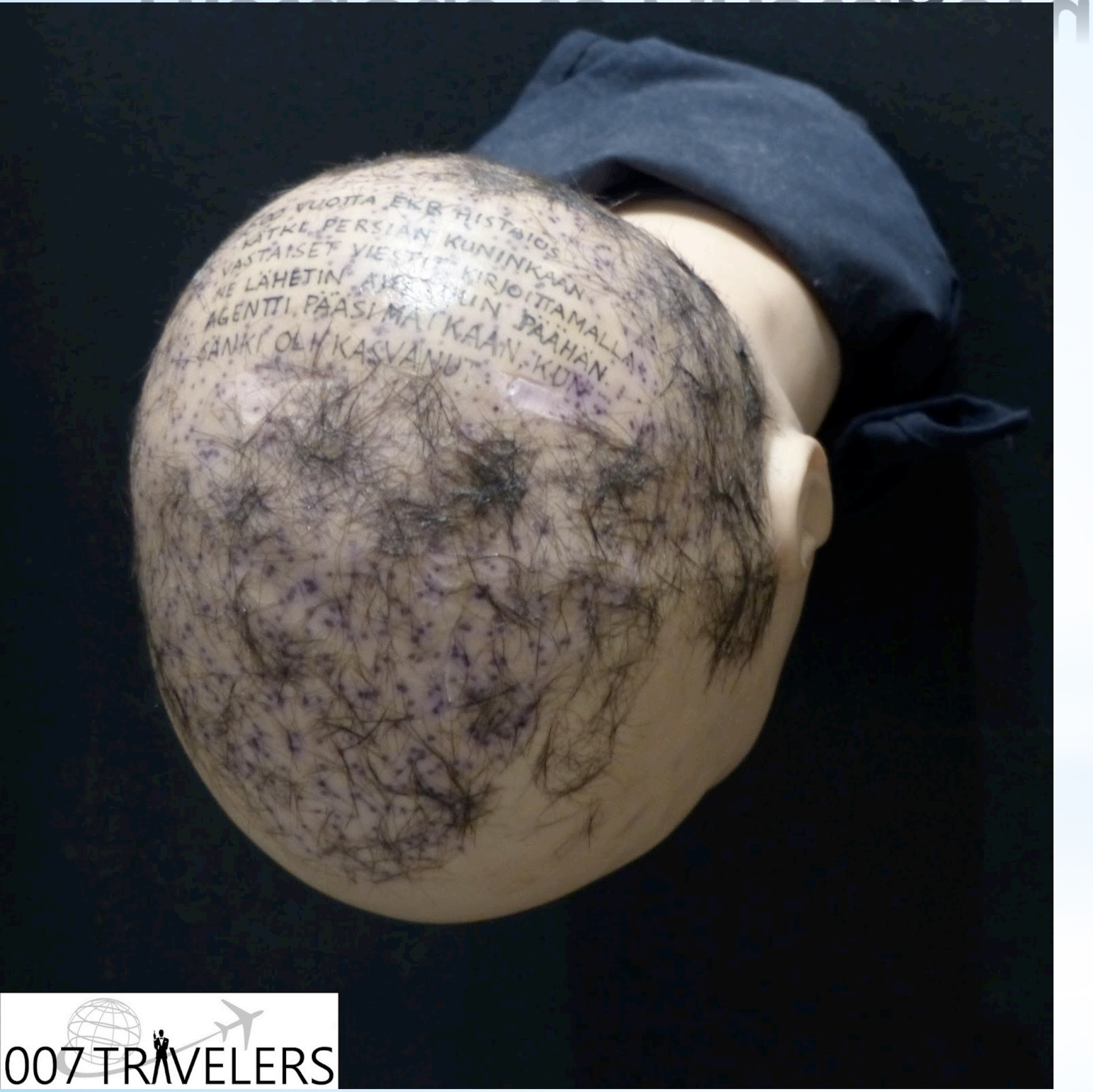
* Cryptography branch of Cryptology

Cryptanalysis (breaking codes)

Steganography (information hiding)

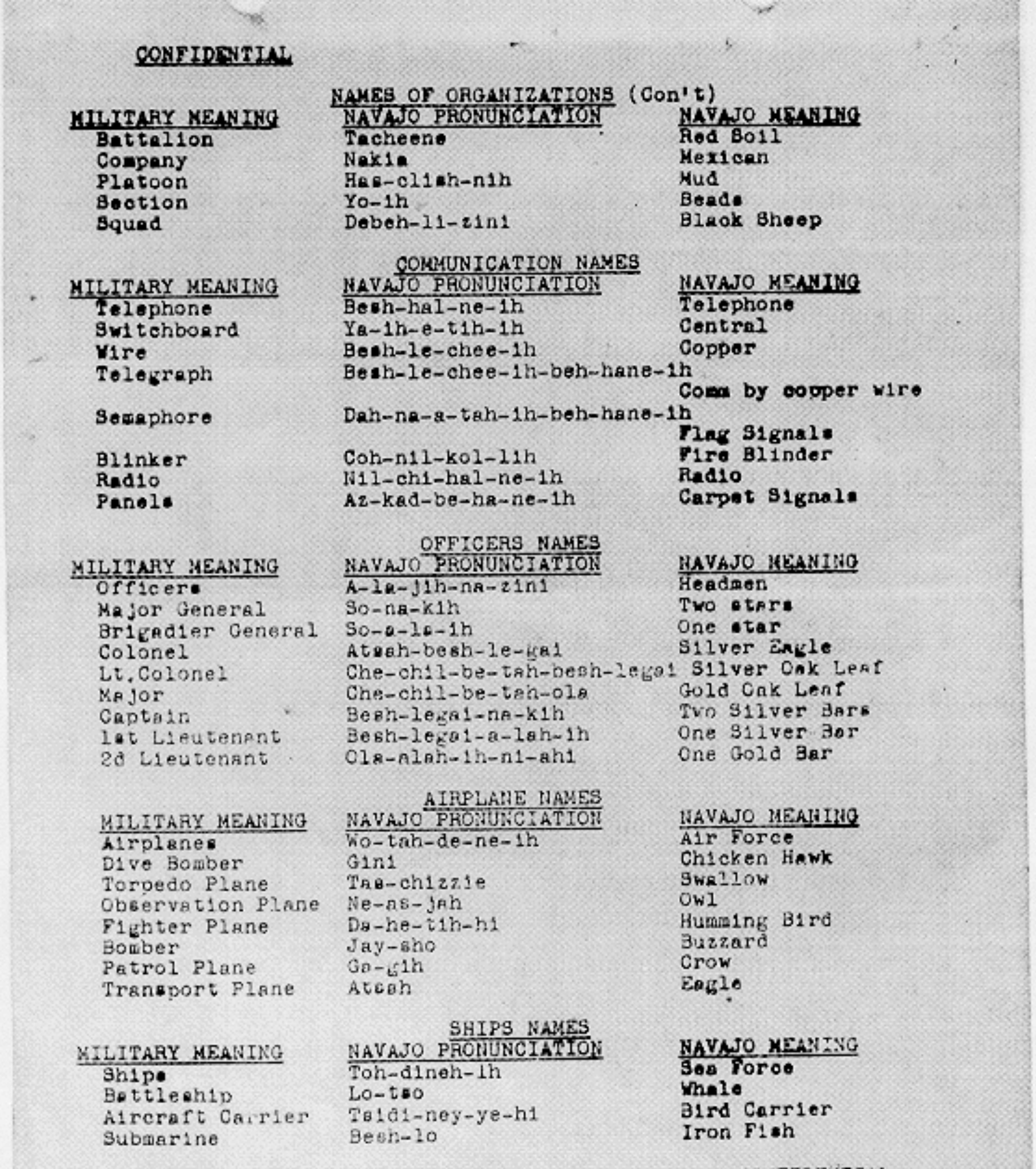
Marius Silaghi, Florida Tech, 2016

*Secret Writing 499 BC Histaeus to Aristagorus


VUOTTA EKR HISTAIOS
KÄTKI PERSIAN KUNINKAAN
VASTAISET VIESTIT KIRJOITTAMALLA
NE LÄHETIN AJELLUN PÄÄHÄN
AGENTTI PÄÄSI MATKAAN, KUN
SÄNKI OLI KASVANUT.
007 TRAVELERS

Persia-Susa / Greece-Miletus

- Navajo code



CONFIDENTIAL

NAMES OF ORGANIZATIONS (Con't)

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Battalion	Tacheene	Red Soil
Company	Nakia	Mexican
Platoon	Has-clish-nih	Mud
Section	Yo-ih	Beads
Squad	Debeh-li-zini	Black Sheep

COMMUNICATION NAMES

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Telephone	Besh-hal-ne-ih	Telephone
Switchboard	Ya-ih-e-tih-ih	Central
Wire	Besh-le-chee-ih	Copper
Telegraph	Besh-le-chee-ih-beh-hane-ih	Comm by copper wire
Semaphore	Dah-na-a-tah-ih-beh-hane-ih	Flag Signals
Blinker	Coh-nil-kol-lih	Fire Blinder
Radio	Nil-chi-hal-ne-ih	Radio
Panels	Az-kad-be-ha-ne-ih	Carpet Signals

OFFICERS NAMES

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Officers	A-la-jih-na-zini	Headmen
Major General	So-na-kih	Two stars
Brigadier General	So-a-la-ih	One star
Colonel	Atsah-besh-le-gai	Silver Eagle
Lt.Colonel	Che-chil-be-tah-besh-legai	Silver Oak Leaf
Major	Che-chil-be-tah-ola	Gold Oak Leaf
Captain	Besh-legai-na-kih	Two Silver Bars
1st Lieutenant	Besh-legai-a-lah-ih	One Silver Bar
2d Lieutenant	Ola-alah-ih-ni-ahi	One Gold Bar

AIRPLANE NAMES

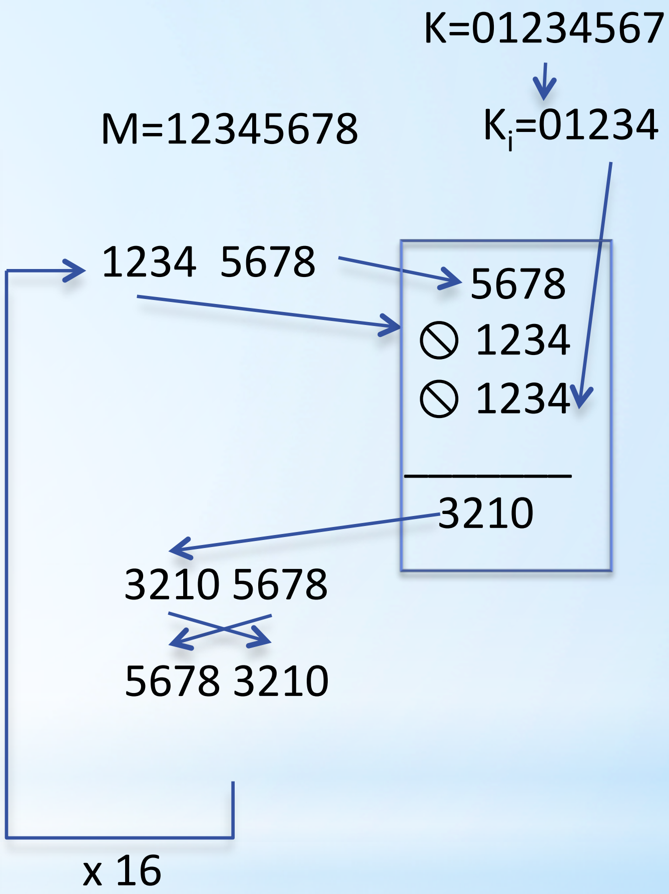
MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Airplanes	Wo-tah-de-ne-ih	Air Force
Dive Bomber	Gini	Chicken Hawk
Torpedo Plane	Tas-chizzie	Swallow
Observation Plane	Ne-as-jah	Owl
Fighter Plane	Da-he-tih-hi	Humming Bird
Bomber	Jay-sho	Buzzard
Patrol Plane	Ga-gih	Crow
Transport Plane	Atsah	Eagle

SHIPS NAMES

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Ships	Toh-dineh-ih	Sea Force
Battleship	Lo-tso	Whale
Aircraft Carrier	Tsidi-ney-ye-hi	Bird Carrier
Submarine	Besh-lo	Iron Fish

"Broken" Data Encryption Standard (DES)

- Created by IBM in 1970s,
- With input from NIST (National Institute for Standards and Technology)
  - Improved resistance to smart attacks
  - Decreased key size
    - 9 characters → 8 characters
    - Breaking in 1 day vs. breaking in 1 year
      - (on a current powerful computer)
  - Cryptanalysis of DES not more powerful than brute force!
  - Legacy: Passwords are often 8 characters.
  - Biggest issue is still: key/password size



K=01234567

M=12345678

K_i=01234

1234 5678

5678

⊘ 1234

⊘ 1234

3210

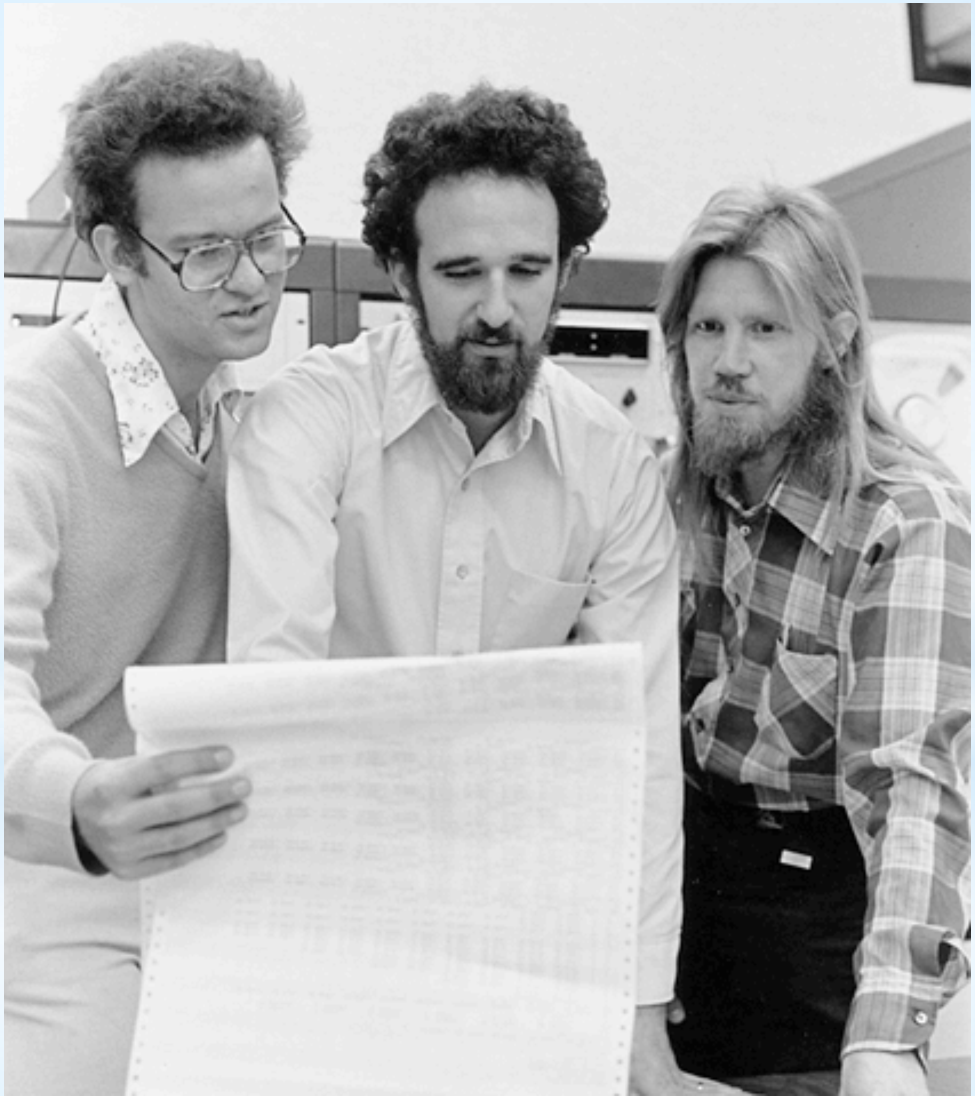
3210 5678

5678 3210

x 16

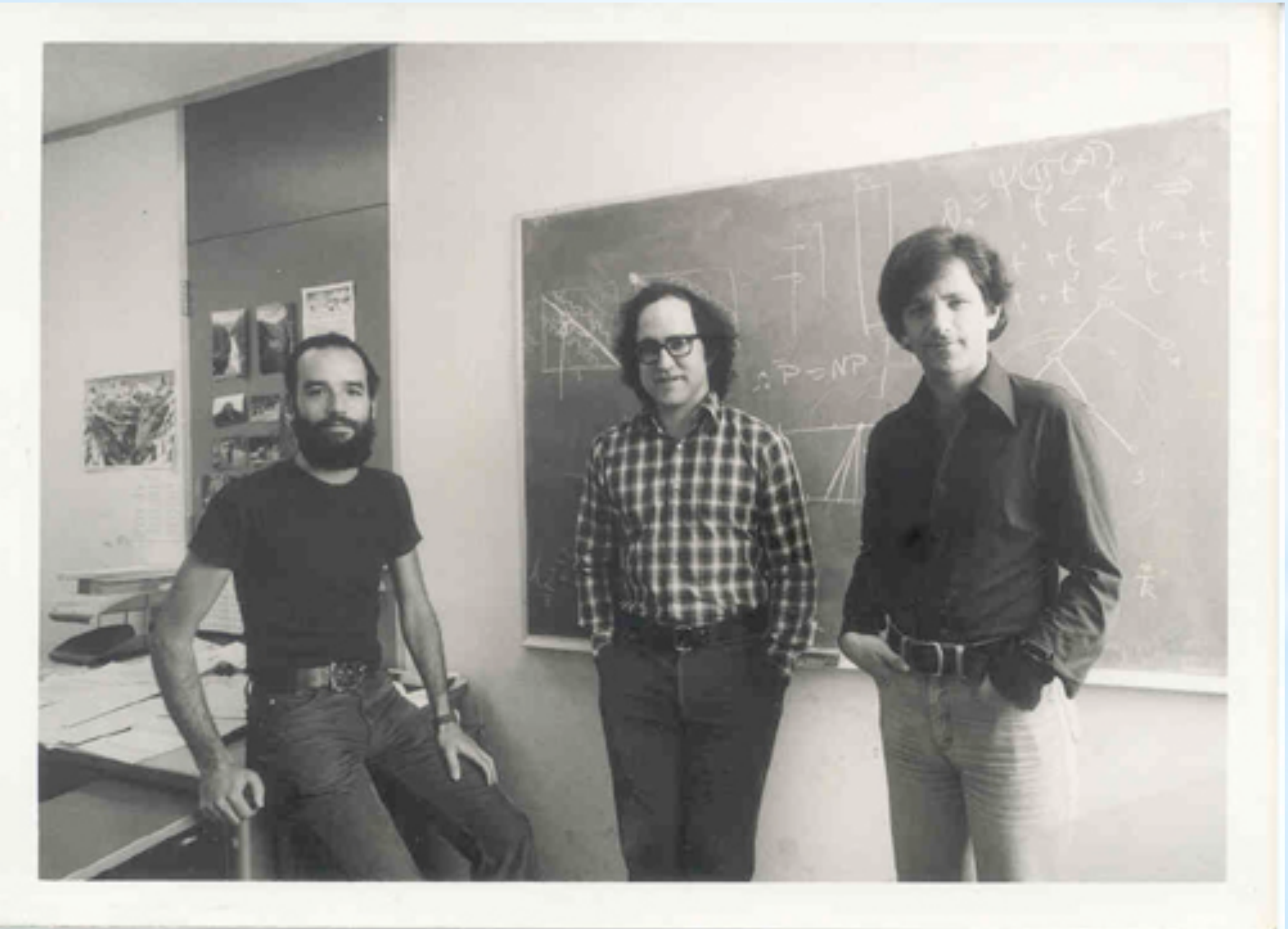
*Diffie-Hellman and Merkle

- *First public techniques for e-commerce (1975,1976)
  - *Key-exchange



*RSA's idea…

RSA (1977) is a technique broadly used over the Internet



*RSA’s idea…

What is the last digit of 3^{2016}?

3^{0} = _____1

3^{1} = _____3

3^{2} = _____9

3^{3} = ____27

3^{4} = ____81

3^{5} = ___243

3^{6} = ___729

3^{7} = _2187

3^{8} = _6561

3^{9} = 19683

____

.

.

.

It repeats…, 3^{2016}=…..?

and ends in 3 at each 3^{4k+1}.

For any x, x^{4k+1} ends in x.

Toy “Encrypt” digits

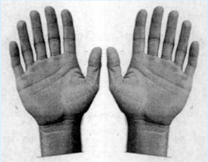
1. Take digit “*x*”
2. ‘Encrypt’: Raise “*x*” to power 3
3. ‘Decrypt’: Raise ciphertext to power 3

x	*y=x³*	*y³=…x*
0	…0	…0
1	…1	…1
2	…8	…2
3	…7	…3
4	…4	…4
5	…5	…5
6	…6	…6
7	…3	…7
8	…2	…8
9	…9	…9

Why does it work? Because: $(x^3)^3=x^9=x^{4*2+1}$

Worried that you can only “encrypt” 10 digits?

What had happened if we had 12 fingers?



- We would count: 1,2,3,4,5,6,7,8,9,α,β,10_{12},11_{12},..
  - one, two,…, nine, dek, el, one dozen, one dozen and one, …

  - Some cultures counted on one hand: 1,2,3,4,10_5,11_5,…
  - Celts/Maya counted on 20 fingers: 61 → 31_{20} (3 scores one)
  - Babylonians counted by 60s:
  - Computers natively commonly count by
    - 2: 1000 → 1111101000_2 = 1(512)+1(256)+1(128)+1(64)+1(32)+1(8)
    - 256: 1000 → $3E8_{256}$ = 3(256s) + 232

  - Computers can count by whatever big number (base) we want…

RSA's idea… continuation

Last digit of 3^x

3^0 = ____1
3^1 = ____3
3^2 = ____9
3^3 = ___27

3^4 = ___81
3^5 = __243
3^6 = __729
3^7 = _2187

3^8 = _6561
3^9 = 19683

______

.

.

.

Repeats…,
and ends in 3 at each 3^{4k+1}.
For any x, x^{4k+1} ends in x.

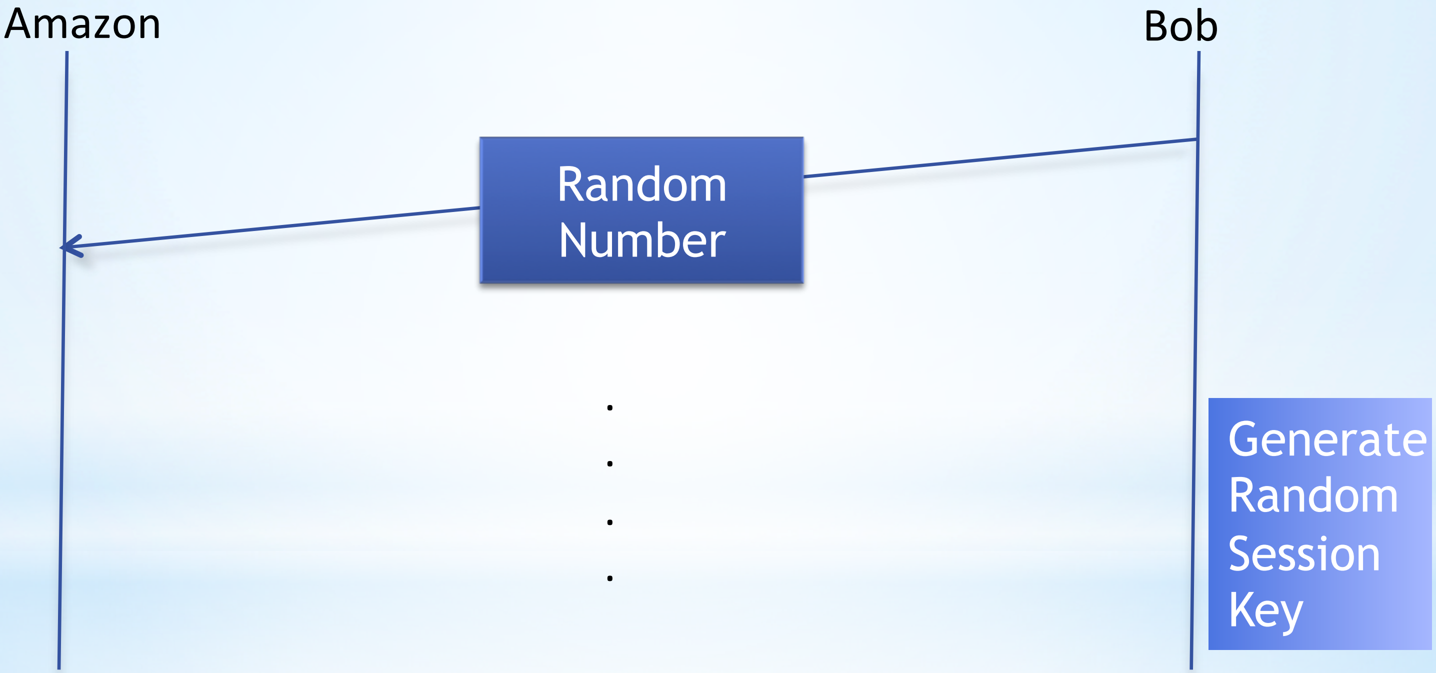
Worried that you can only "encrypt" 10 digits?

Use a higher base!

- If base is N=p*q, then input repeated at (p-1)(q-1)k+1
  - 10(2*5), (2-1)(5-1)=4→4k+1
    1. Take 'digit' "*x*"
    2. 'Encrypt': Raise "*x*" to power 3
    3. 'Decrypt': Raise secret to power ?
       - 3 * ? = 4k+1
       - 3 * 3 = 9 = 4 * 2 + 1
  - 187(11*17)→10*16k+1=160k+1
    - 3*? = 160k+1
    - 160 * 1 + 1 = 161 :3…
    - 160 * 2 + 1 = 321 :3=107
    - $((x)^3)^{107} = (x)^{321} = (x)^{160*2+1} =$ …x
- Without knowing p and q (N=p * q)
  - 3*? = ?k+1

*Random Numbers: Attacks

Known issue: avoid frequent keys and passwords: “12345678”, “password”, “qwertyui”. For security, secret keys have to be **random**.



After seeing a random number, it should be impossible to guess the next random number….

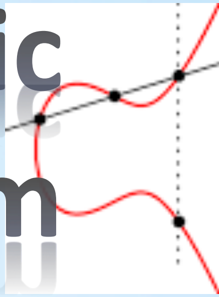
Marius Silaghi, Florida Tech, 2016

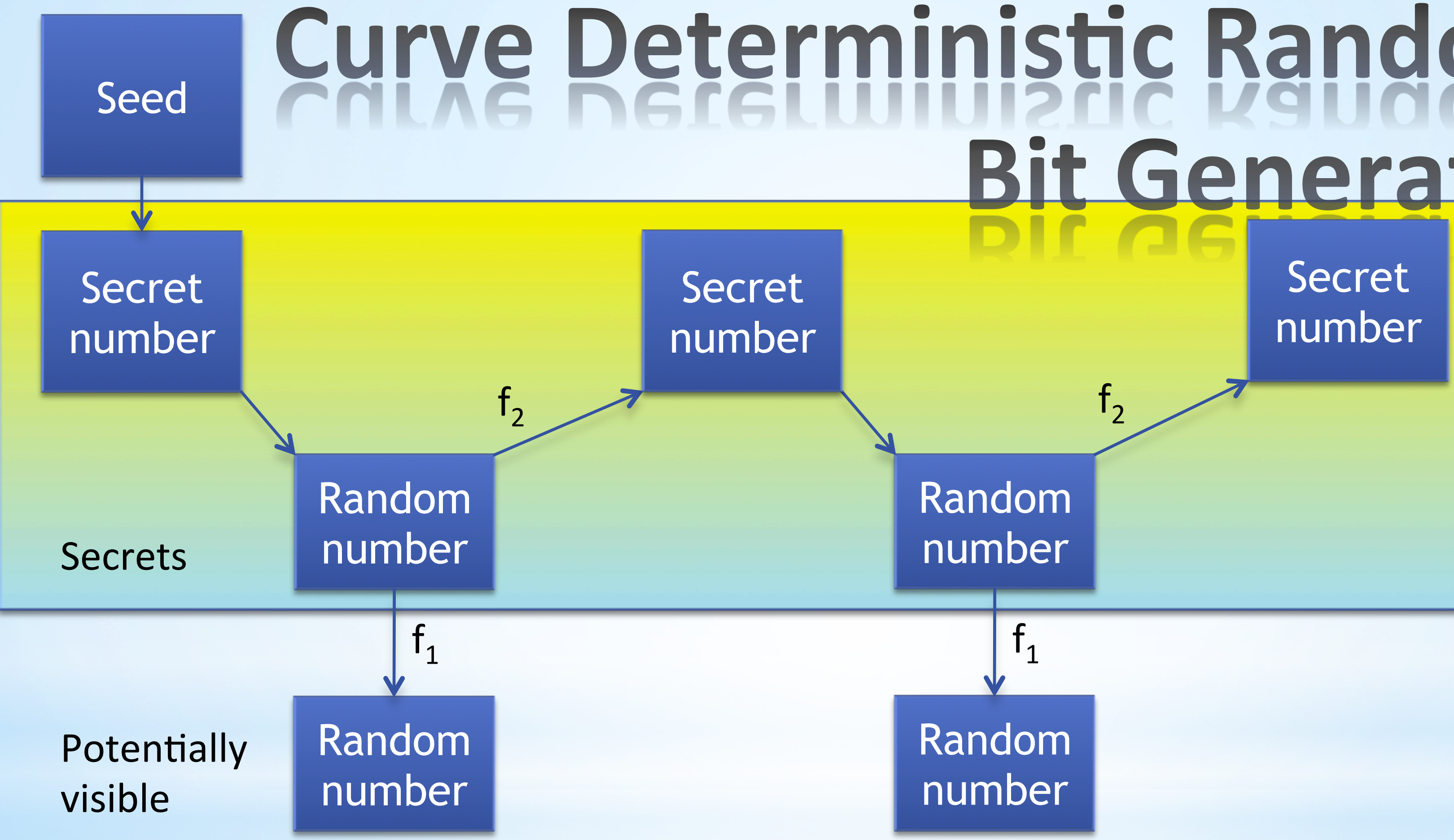
Random numbers in computers

- Generating numbers between 1 and 9
- Next_X = sum_digits(sum_digits (4 * X + 2))

- X = 1   (seed)
- X = 6   sum_digits(4 * 1 + 2 = 6)
- X = 8   sum_digits(4 * 6 + 2 = 24 + 2 = 26)
- X = 7   sum_digits(4 * 8 + 2 = 32 + 2 = 34)
- X = 3   sum_digits(4 * 7 + 2 = 28 + 2 = 30)
- X = 5   sum_digits(4 * 3 + 2 = 12 + 2 = 14)
- X = 4   sum_digits(4 * 5 + 2 = 20 + 2 = 22)
- X = 9   sum_digits(4 * 4 + 2 = 16 + 2 = 18)
- X = 2   sum_digits(sum_digits(4 * 9 + 2 = 36 + 2 = 38) = 11)
- X = 1   sum_digits(4 * 2 + 2 = 8 + 2 = 10)

*Backdoor?! in the Dual Elliptic Curve Deterministic Random Bit Generator





Seed

Secret number

Secret number

Secret number

Random number

Random number

Secrets

f_2

f_2

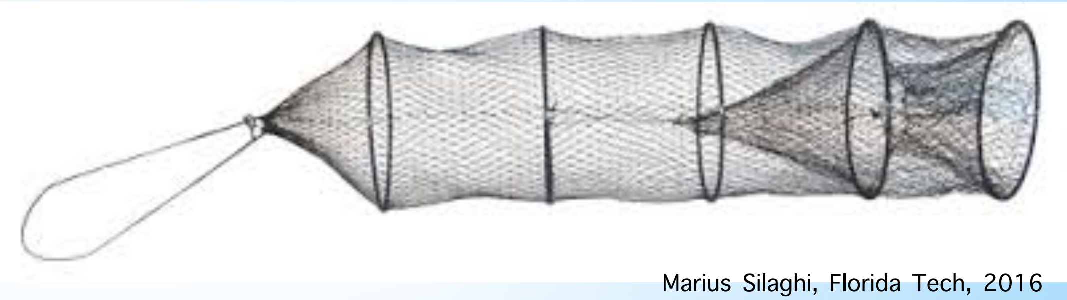
f_1

f_1

Potentially visible

Random number

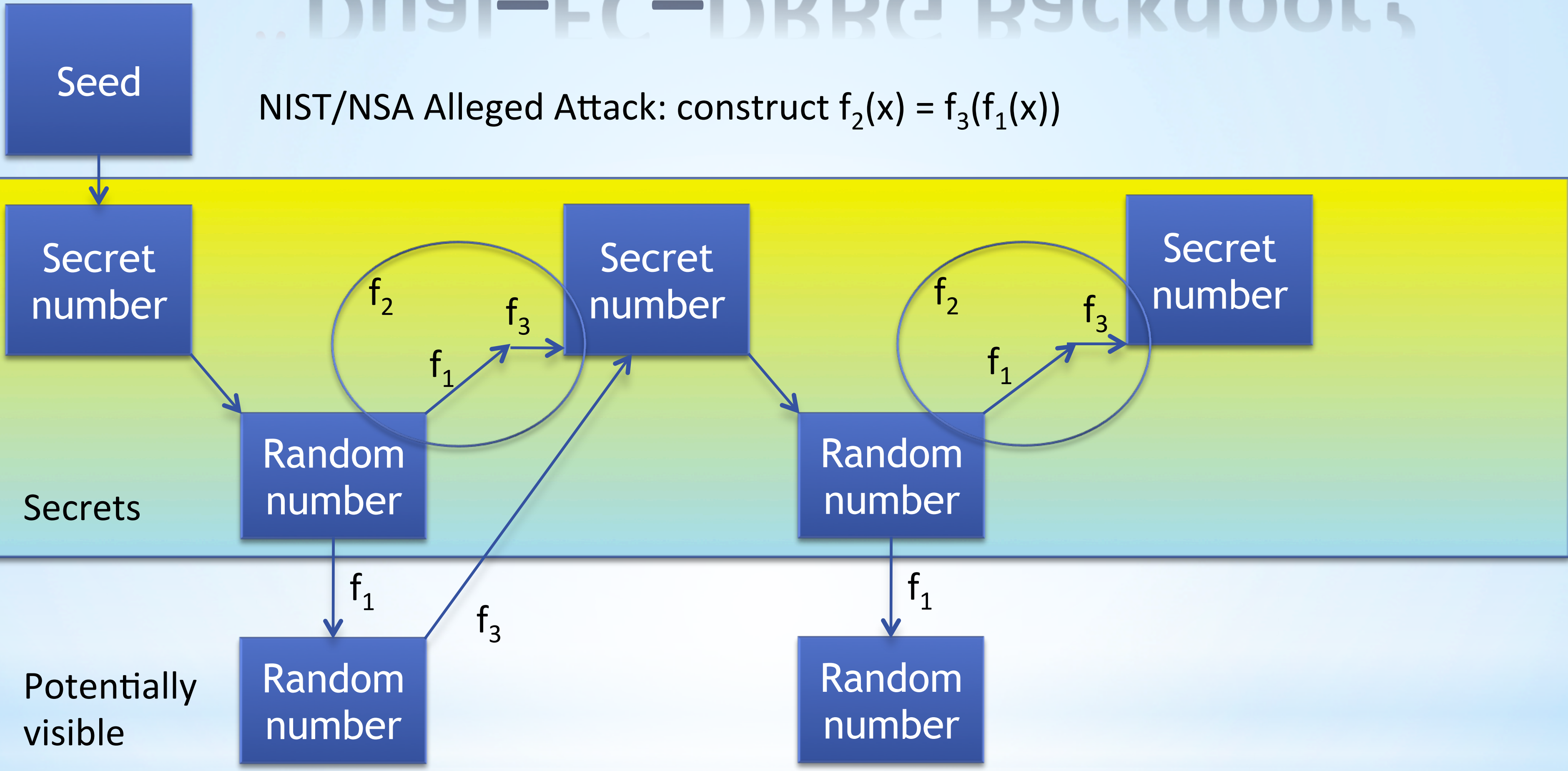
Random number



Where f_1 and f_2 are one-way functions

Dual_EC_DRBG Backdoor?

NIST/NSA Alleged Attack: construct $f_2(x) = f_3(f_1(x))$



Idea of backdoor published in 1997 (and patented in 2005).

Suspected Backdoor standardized by NIST in 2000-2005.

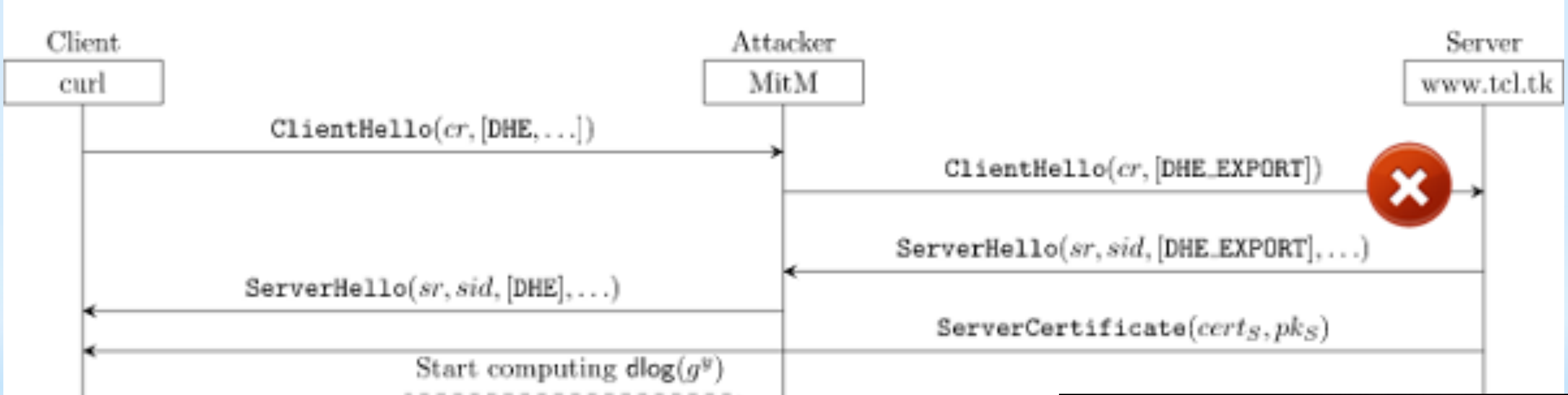
Researchers complain in 2006, 2007 (complains not heeded by anyone).

NSA paid? RSA Security 10 millions to make Dual_EC_DRBG first choice in its software in 2004?

Alleged scheme described by Snowden leaks in 2013.

Logjam TLS Attack (2015)

- First, coax servers to use (commonly disabled) DHE-EXPORT cipher
  - A cipher installed in 1990s when export restrictions required keys to be smaller than 512 bits


Client
curl
Attacker
MitM
Server
www.tcl.tk
ClientHello(cr, [DHE, . . .])
ClientHello(cr, [DHE_EXPORT])
ServerHello(sr, sid, [DHE_EXPORT], . . .)
ServerHello(sr, sid, [DHE], . . .)
ServerCertificate($certs_S, pk_S$)
Start computing dlog(g^y)

  - 2 primes of 512 bits are used 92.3% of sites
  - Can in advance build a “kind of logarithm table”

*What makes a backdoor/bug so dangerous?

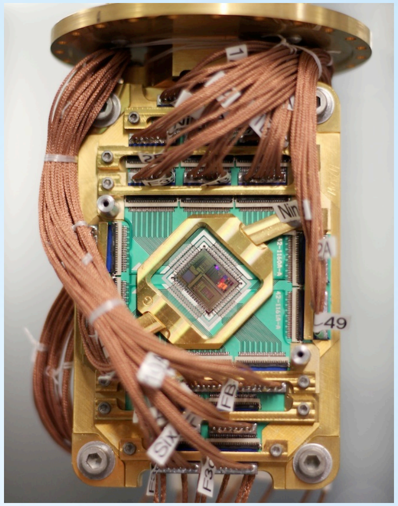
- Cryptography textbooks and authors recommend students to:
  - “never implement your own algorithms”,
  - but to use only widely used libraries ☺

- Officially the reason is that:
  - Widely used libraries have been more tested and are more likely to be clean of bugs.
  - Cryptography is difficult and likely novices will do it wrong.

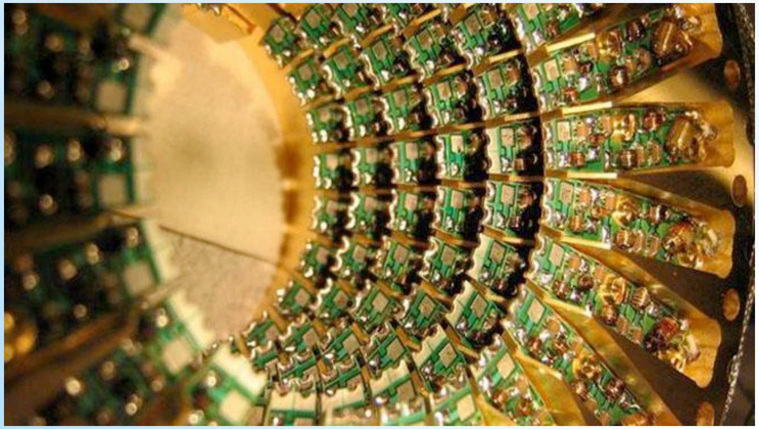
- Practically:
  - Needed for **Federal Information Processing Standards** (FIPS) certification (government required)
  - And it is easier to maintain one product, then two.

- So, a few backdoors/bugs in RSA or OpenSSL libraries are sufficient to control most users. ☹
  - Heartbleed, Logjam TLS, Dual_EC_DRBG

Future Quantum Computers

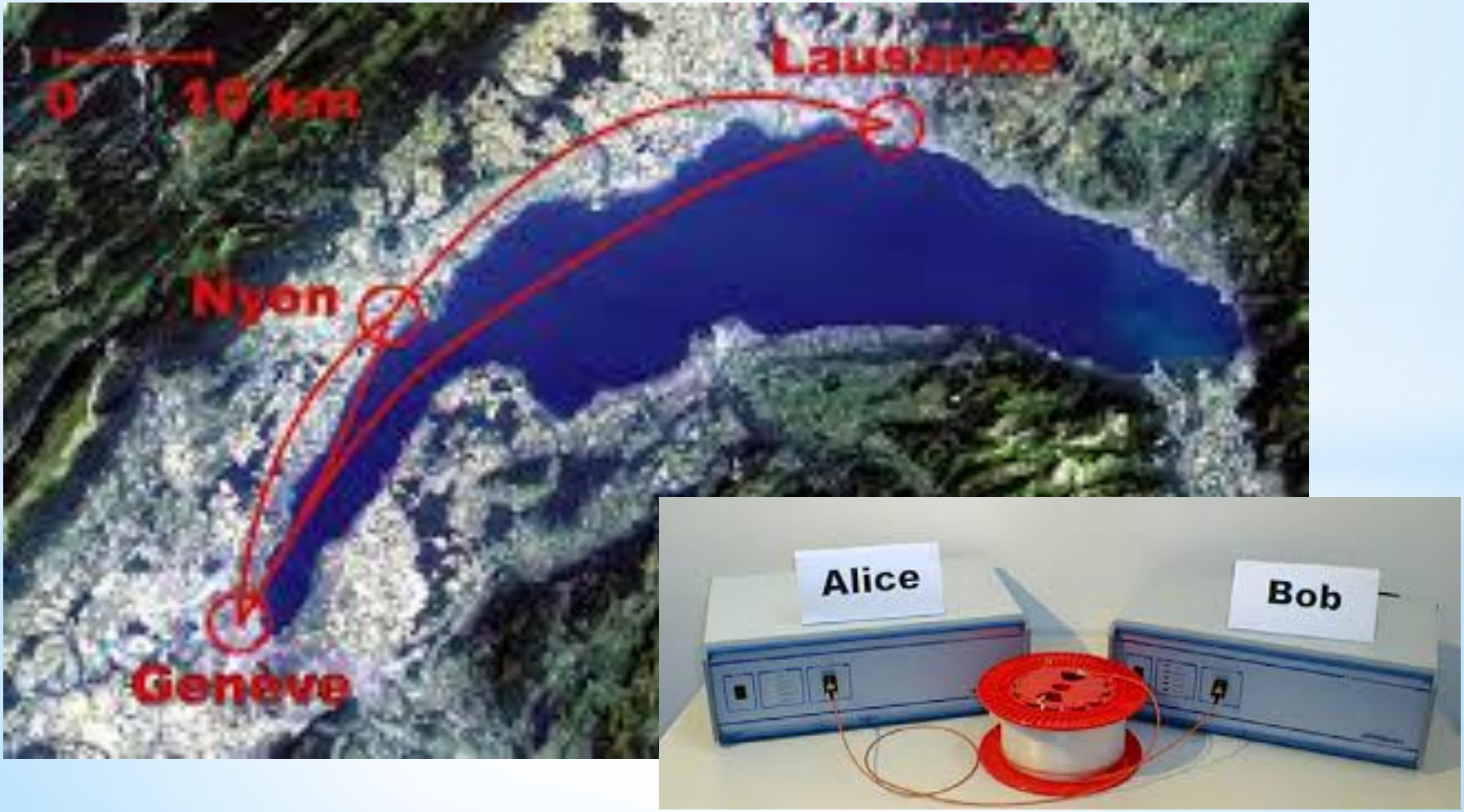


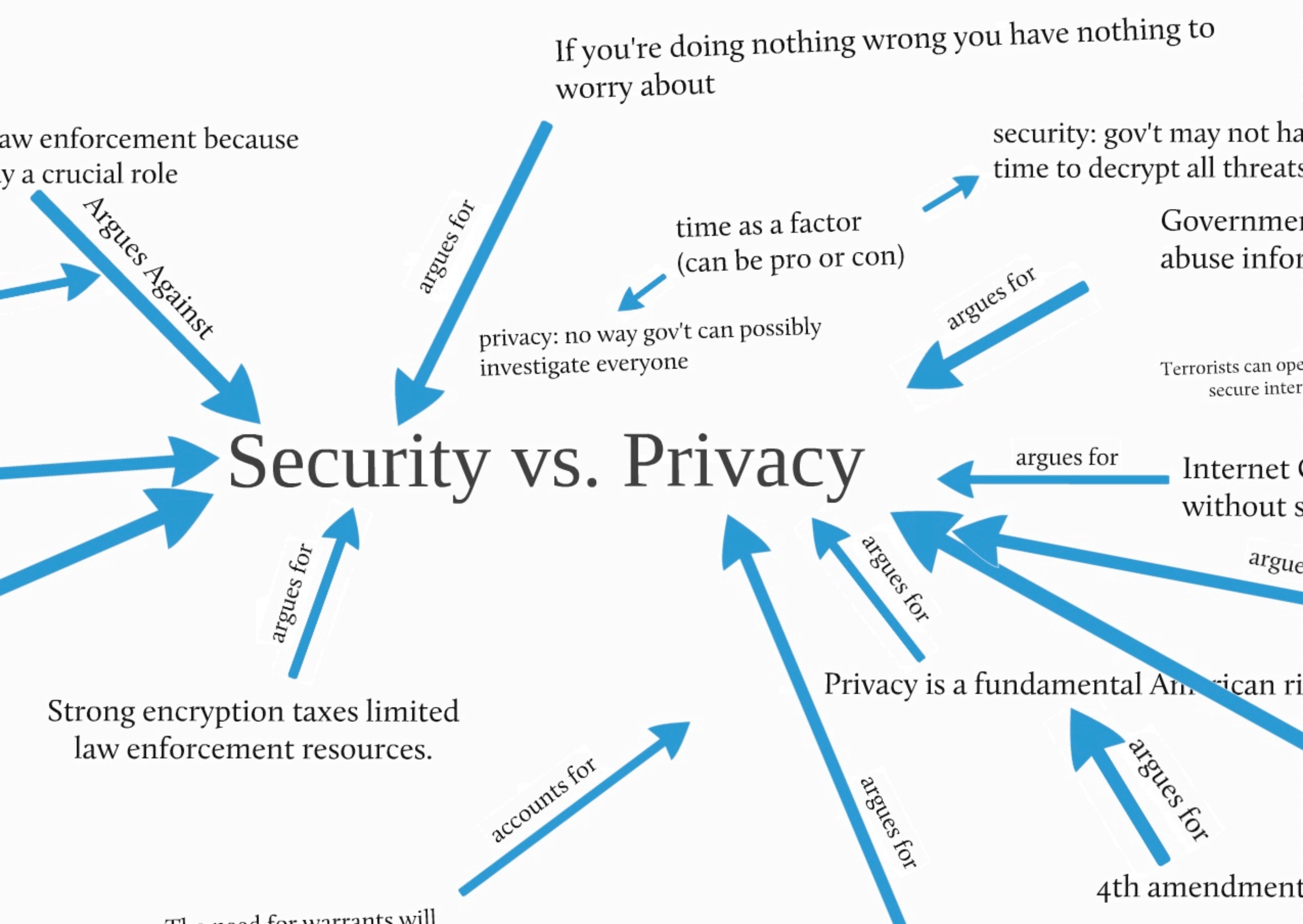
- Are they here?
- What would they change?
- Does NSA already own one?



*Quantum Cryptography

- *2002, 67 km Quantum key distribution





If you're doing nothing wrong you have nothing to worry about

aw enforcement because
y a crucial role

security: gov't may not ha
time to decrypt all threats

Argues Against

argues for

time as a factor
(can be pro or con)

Governmen
abuse infor

argues for

privacy: no way gov't can possibly investigate everyone

Terrorists can ope
secure inter

Security vs. Privacy

argues for

Internet
without s

argues for

argues for

argue

Privacy is a fundamental American ri

Strong encryption taxes limited law enforcement resources.

accounts for

argues for

argues for

4th amendment

The need for warrants will

*Cryptography's problems

January 24, 2012:   US vs. Fricosu

Colorado Woman Ordered to Decrypt Laptop in Bank Fraud Case

Colorado U.S. District Judge Robert Blackburn said the Fifth Amendment does not protect her from the order