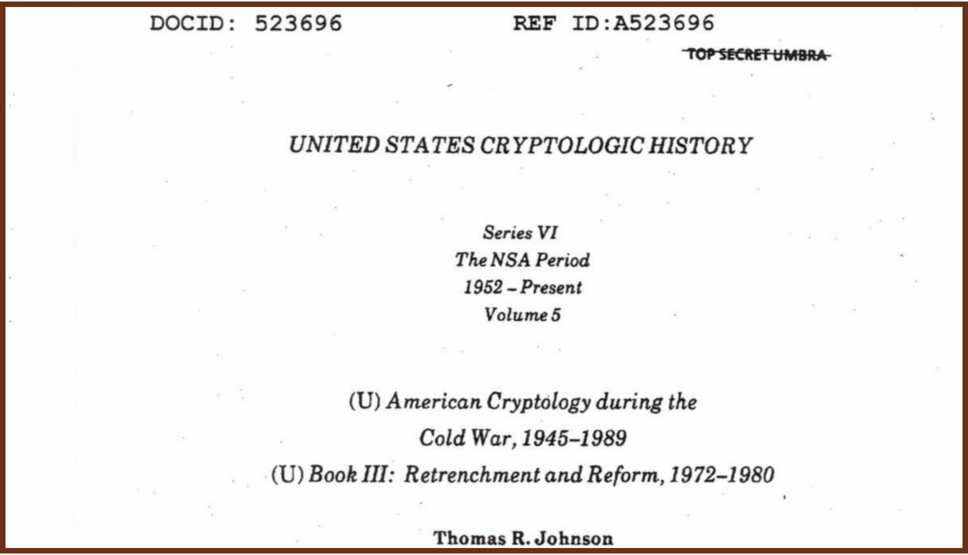
NSA’s influence on cryptographic standards

Daniel J. Bernstein

University of Illinois at Chicago;
Ruhr University Bochum

One of NSA’s secret history books



DOCID: 523696 REF ID:A523696

~~TOP SECRET UMBRA~~

UNITED STATES CRYPTOLOGIC HISTORY

Series VI
The NSA Period
1952 – Present
Volume 5

(U) *American Cryptology during the*
Cold War, 1945–1989
(U) *Book III: Retrenchment and Reform, 1972–1980*

Thomas R. Johnson

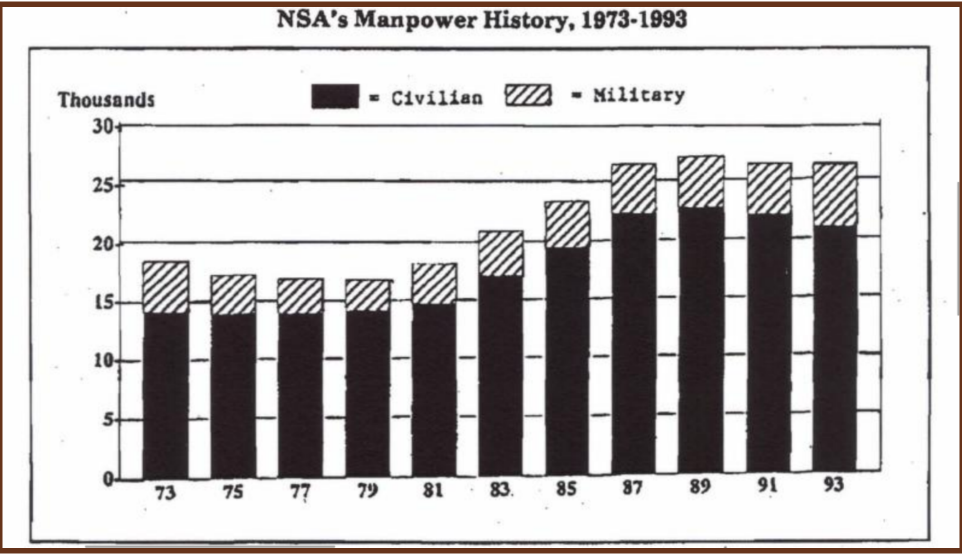
Why is this no longer secret?

Two organizations filed official requests:

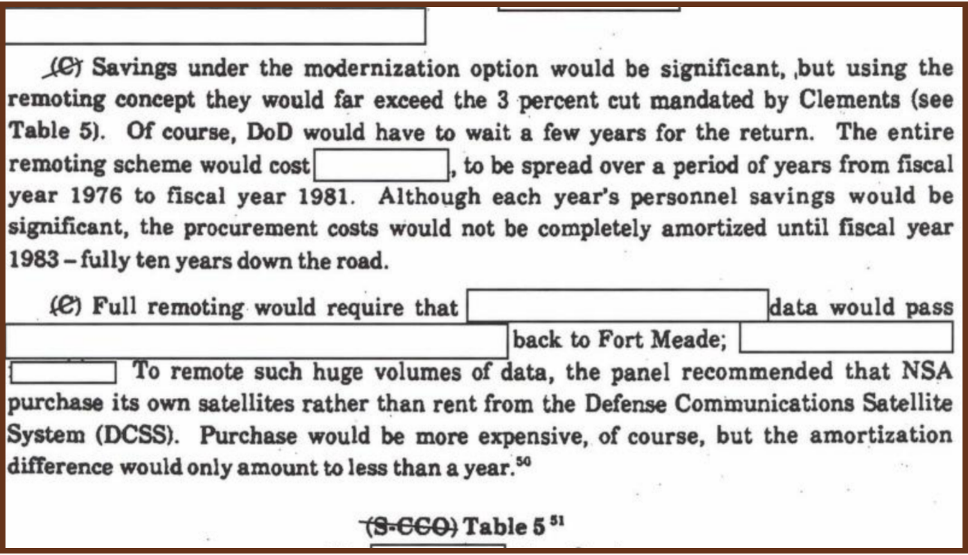
- George Washington University's National Security Archive heard about existence of this book; filed declassification requests and appeals starting in 2006.
- Cryptome (John Young, Deborah Natsios) filed Freedom of Information Act (FOIA) request in 2009 re 1977 "Meyer letter".

These requests eventually led to release of the book—minus some still-classified parts.

NSA grows beyond 25000 people



Equipment: e.g., satellites



[redacted] [redacted]

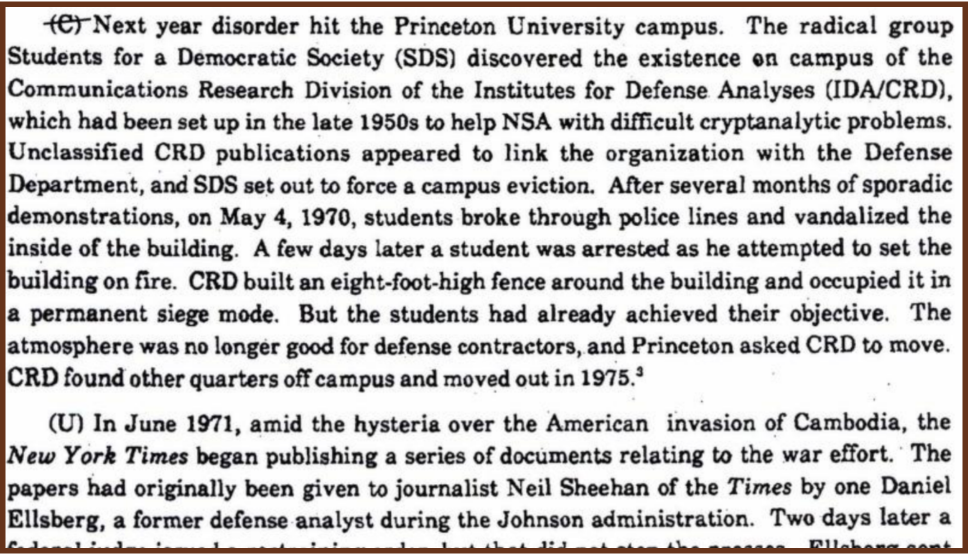
~~(C)~~ Savings under the modernization option would be significant, but using the remoting concept they would far exceed the 3 percent cut mandated by Clements (see Table 5). Of course, DoD would have to wait a few years for the return. The entire remoting scheme would cost [redacted], to be spread over a period of years from fiscal year 1976 to fiscal year 1981. Although each year's personnel savings would be significant, the procurement costs would not be completely amortized until fiscal year 1983 – fully ten years down the road.

~~(C)~~ Full remoting would require that [redacted] data would pass [redacted] back to Fort Meade; [redacted] [redacted] To remote such huge volumes of data, the panel recommended that NSA purchase its own satellites rather than rent from the Defense Communications Satellite System (DCSS). Purchase would be more expensive, of course, but the amortization difference would only amount to less than a year.[50]

~~(S-CCO)~~ Table 5[51]

[redacted]

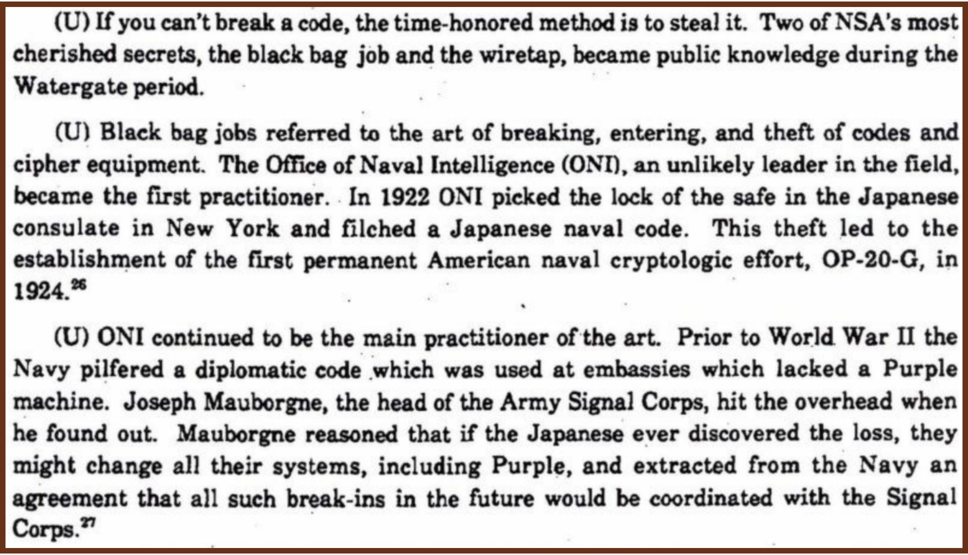
Defense contractors: e.g., IDA



~~(C)~~ Next year disorder hit the Princeton University campus. The radical group Students for a Democratic Society (SDS) discovered the existence on campus of the Communications Research Division of the Institutes for Defense Analyses (IDA/CRD), which had been set up in the late 1950s to help NSA with difficult cryptanalytic problems. Unclassified CRD publications appeared to link the organization with the Defense Department, and SDS set out to force a campus eviction. After several months of sporadic demonstrations, on May 4, 1970, students broke through police lines and vandalized the inside of the building. A few days later a student was arrested as he attempted to set the building on fire. CRD built an eight-foot-high fence around the building and occupied it in a permanent siege mode. But the students had already achieved their objective. The atmosphere was no longer good for defense contractors, and Princeton asked CRD to move. CRD found other quarters off campus and moved out in 1975.[3]

(U) In June 1971, amid the hysteria over the American invasion of Cambodia, the *New York Times* began publishing a series of documents relating to the war effort. The papers had originally been given to journalist Neil Sheehan of the *Times* by one Daniel Ellsberg, a former defense analyst during the Johnson administration. Two days later a federal judge issued a restraining order, but that did not stop the process. Ellsberg sent

Breaking encryption, *quietly*

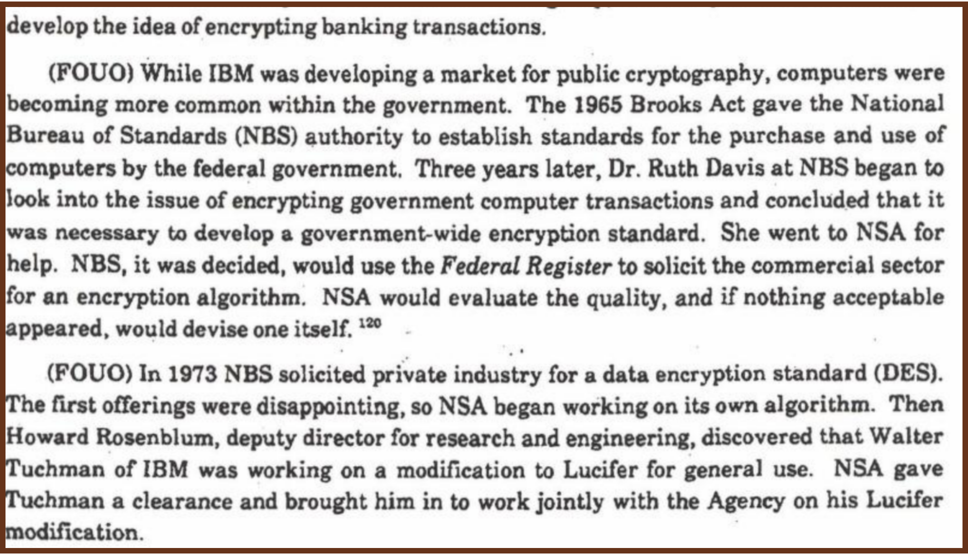


(U) If you can't break a code, the time-honored method is to steal it. Two of NSA's most cherished secrets, the black bag job and the wiretap, became public knowledge during the Watergate period.

(U) Black bag jobs referred to the art of breaking, entering, and theft of codes and cipher equipment. The Office of Naval Intelligence (ONI), an unlikely leader in the field, became the first practitioner. In 1922 ONI picked the lock of the safe in the Japanese consulate in New York and filched a Japanese naval code. This theft led to the establishment of the first permanent American naval cryptologic effort, OP-20-G, in 1924.[26]

(U) ONI continued to be the main practitioner of the art. Prior to World War II the Navy pilfered a diplomatic code which was used at embassies which lacked a Purple machine. Joseph Mauborgne, the head of the Army Signal Corps, hit the overhead when he found out. Mauborgne reasoned that if the Japanese ever discovered the loss, they might change all their systems, including Purple, and extracted from the Navy an agreement that all such break-ins in the future would be coordinated with the Signal Corps.[27]

Working with NBS (NIST) and IBM

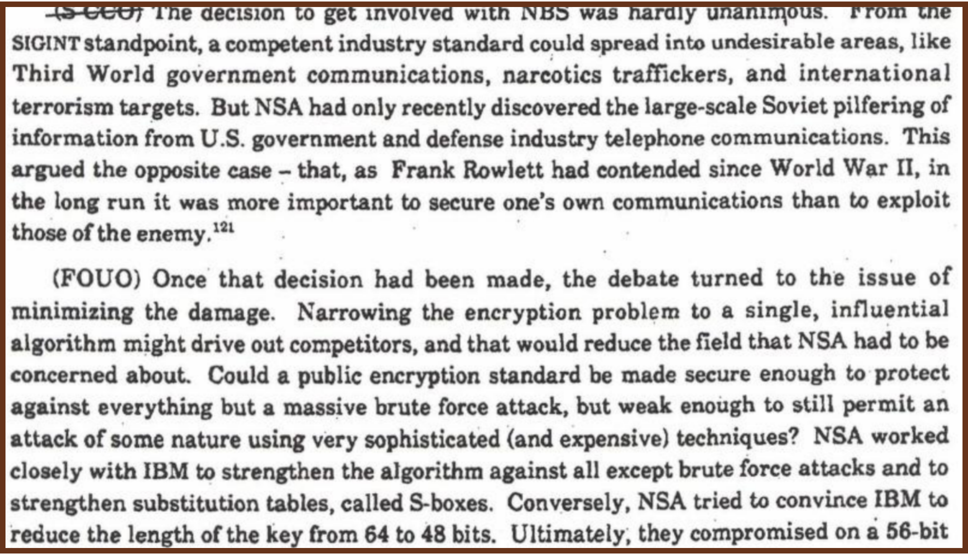


develop the idea of encrypting banking transactions.

(FOUO) While IBM was developing a market for public cryptography, computers were becoming more common within the government. The 1965 Brooks Act gave the National Bureau of Standards (NBS) authority to establish standards for the purchase and use of computers by the federal government. Three years later, Dr. Ruth Davis at NBS began to look into the issue of encrypting government computer transactions and concluded that it was necessary to develop a government-wide encryption standard. She went to NSA for help. NBS, it was decided, would use the *Federal Register* to solicit the commercial sector for an encryption algorithm. NSA would evaluate the quality, and if nothing acceptable appeared, would devise one itself. [120]

(FOUO) In 1973 NBS solicited private industry for a data encryption standard (DES). The first offerings were disappointing, so NSA began working on its own algorithm. Then Howard Rosenblum, deputy director for research and engineering, discovered that Walter Tuchman of IBM was working on a modification to Lucifer for general use. NSA gave Tuchman a clearance and brought him in to work jointly with the Agency on his Lucifer modification.

The decision to sabotage DES



~~(S-CCO)~~ The decision to get involved with NBS was hardly unanimous. From the SIGINT standpoint, a competent industry standard could spread into undesirable areas, like Third World government communications, narcotics traffickers, and international terrorism targets. But NSA had only recently discovered the large-scale Soviet pilfering of information from U.S. government and defense industry telephone communications. This argued the opposite case – that, as Frank Rowlett had contended since World War II, in the long run it was more important to secure one's own communications than to exploit those of the enemy.[121]

(FOUO) Once that decision had been made, the debate turned to the issue of minimizing the damage. Narrowing the encryption problem to a single, influential algorithm might drive out competitors, and that would reduce the field that NSA had to be concerned about. Could a public encryption standard be made secure enough to protect against everything but a massive brute force attack, but weak enough to still permit an attack of some nature using very sophisticated (and expensive) techniques? NSA worked closely with IBM to strengthen the algorithm against all except brute force attacks and to strengthen substitution tables, called S-boxes. Conversely, NSA tried to convince IBM to reduce the length of the key from 64 to 48 bits. Ultimately, they compromised on a 56-bit

Making standards weak enough

> “Narrowing the encryption problem to a single, influential algorithm might **drive out competitors**, and that would reduce the field that NSA had to be concerned about. Could a **public encryption standard** be made secure enough to protect against everything but a massive brute force attack, but **weak enough to still permit an attack of some nature** using very sophisticated (and expensive) techniques?” (Emphasis added.)

DES sabotage: key too small

> "NSA gave Tuchman a clearance and brought him in to **work jointly with the Agency** on his Lucifer modification. . . . **NSA tried to convince IBM to reduce the length of the key from 64 to 48 bits.** Ultimately, they compromised on a 56-bit key. . . . NSA scientists working the problem crossed back and forth between the two agencies [NSA and NBS], and **NSA unquestionably exercised an influential role in the algorithm**." (Emphasis added.)

Telling the public a different story

1978 Tuchman interview, Cryptologia vol. 2:

- DES was “the culmination of six years of research and development at IBM”.
- Re accusations IBM+NSA had “conspired”: “We developed the DES algorithm entirely within IBM using IBMers. The NSA did not dictate a single wire!”

1979 NSA director: “NSA has been accused of intervening in the development of the DES and of tampering with the standard so as to weaken it cryptographically. This allegation is totally false.”

1990s: Digital Signature Standard

1991.08: NIST issues Federal Register notice announcing DSS.

1991.08: Computer Professionals for Social Responsibility files FOIA request.

1991.10: CPSR appeals FOIA denial.

1992.04: CPSR files FOIA lawsuit.

1990s: Digital Signature Standard

1991.08: NIST issues Federal Register notice announcing DSS.

1991.08: Computer Professionals for Social Responsibility files FOIA request.

1991.10: CPSR appeals FOIA denial.

1992.04: CPSR files FOIA lawsuit.

1992.06: FOIA response admits there are 142 pages from NIST + 1138 from NSA.

1993.04: FOIA documents indicate that NSA dominated the DSS design.

DSS (DSA) weaknesses

Most obvious problem: Key too small, given public algorithms to attack “discrete logs”.

DSS (DSA) weaknesses

Most obvious problem: Key too small, given public algorithms to attack “discrete logs”.

More subtle concerns:

- These algorithms were new, complicated. (Unsurprisingly, later superseded.)
- After breaking one target, can quickly break more. (Exploited in, e.g., Logjam.)
- Pitfalls would trap implementors. (Exploited in Sony PS3 ECDSA attack.)
- There could be back doors. (Disputed at the time but later shown feasible.)

2000s: Dual EC

2005.12: NIST issues a draft standard for random-number generators, including Dual EC.

2006.03: An attack algorithm shows that Dual EC is not a secure RNG. See also second attack algorithm.

2000s: Dual EC

2005.12: NIST issues a draft standard for random-number generators, including Dual EC.

2006.03: An attack algorithm shows that Dual EC is not a secure RNG. See also second attack algorithm.

2006.06: NIST publishes final standard, including Dual EC.

2000s: Dual EC

2005.12: NIST issues a draft standard for random-number generators, including Dual EC.

2006.03: An attack algorithm shows that Dual EC is not a secure RNG. See also second attack algorithm.

2006.06: NIST publishes final standard, including Dual EC.

2007.08: Another attack algorithm shows that Dual EC is backdoorable.

2008–2013: NIST approves 73 Dual EC products.

2013: Snowden

2013.09: New York Times report says “Classified N.S.A. memos appear to confirm that the fatal weakness, discovered by two Microsoft cryptographers in 2007, was engineered by the agency. The N.S.A. wrote the standard and aggressively pushed it on the international group, privately calling the effort ‘a challenge in finesse.’ ”

2013.12: Reuters report says NSA paid RSA $10,000,000 to switch to Dual EC.

SIGINT Enabling Project

$275,400,000 budget in 2012 fiscal year.

“The SIGINT Enabling Project actively engages the US and foreign IT industries to **covertly influence and/or overtly leverage** their commercial products’ designs. These design changes **make the systems in question exploitable** . . . To the consumer and other adversaries, however, the systems’ security remains intact.” (Emphasis added.)

SIGINT Enabling Project, part 2

“**Influence policies, standards and specification** for commercial public key technologies. . . . **Shape the worldwide commercial cryptography marketplace** to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS.” (Emphasis added.)

SIGINT Enabling Project, part 2

"**Influence policies, standards and specification** for commercial public key technologies. … **Shape the worldwide commercial cryptography marketplace** to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS." (Emphasis added.)

Why is this no longer secret? Snowden.

People paying attention pre-Snowden already understood *roughly* what was happening, but Snowden made the picture much more clear.

Imagine yourself as the attacker

You have a very large budget to intercept communication worldwide, and to “covertly influence and/or overtly leverage” deployed crypto to make it “exploitable”.

What do you do?

Imagine yourself as the attacker

You have a very large budget to intercept communication worldwide, and to “covertly influence and/or overtly leverage” deployed crypto to make it “exploitable”.

What do you do? Here are some ideas:

- Hire mathematicians to break crypto for you—and to stay quiet about it.

Imagine yourself as the attacker

You have a very large budget to intercept communication worldwide, and to “covertly influence and/or overtly leverage” deployed crypto to make it “exploitable”.

What do you do? Here are some ideas:

- Hire mathematicians to break crypto for you—and to stay quiet about it.
- Use legal threats to discourage publication of strong crypto.

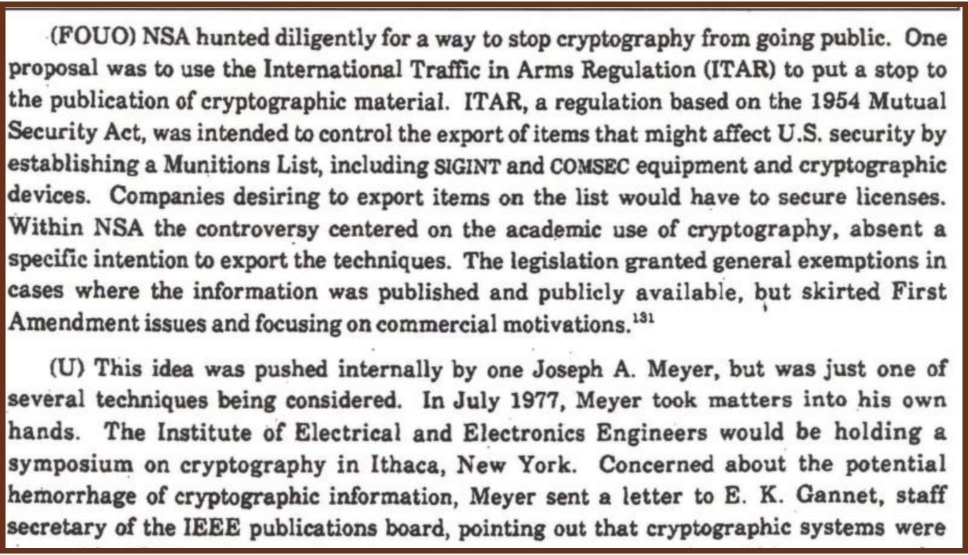
Imagine yourself as the attacker

You have a very large budget to intercept communication worldwide, and to “covertly influence and/or overtly leverage” deployed crypto to make it “exploitable”.

What do you do? Here are some ideas:

- Hire mathematicians to break crypto for you—and to stay quiet about it.
- Use legal threats to discourage publication of strong crypto.
- Attract people to cryptosystems that you secretly know how to break.

Export laws vs. strong crypto



(FOUO) NSA hunted diligently for a way to stop cryptography from going public. One proposal was to use the International Traffic in Arms Regulation (ITAR) to put a stop to the publication of cryptographic material. ITAR, a regulation based on the 1954 Mutual Security Act, was intended to control the export of items that might affect U.S. security by establishing a Munitions List, including SIGINT and COMSEC equipment and cryptographic devices. Companies desiring to export items on the list would have to secure licenses. Within NSA the controversy centered on the academic use of cryptography, absent a specific intention to export the techniques. The legislation granted general exemptions in cases where the information was published and publicly available, but skirted First Amendment issues and focusing on commercial motivations.[131]

(U) This idea was pushed internally by one Joseph A. Meyer, but was just one of several techniques being considered. In July 1977, Meyer took matters into his own hands. The Institute of Electrical and Electronics Engineers would be holding a symposium on cryptography in Ithaca, New York. Concerned about the potential hemorrhage of cryptographic information, Meyer sent a letter to E. K. Gannet, staff secretary of the IEEE publications board, pointing out that cryptographic systems were

1990s: my first lawsuit

NSA denies my request to publish.
I ask court to declare that this censorship violates the U.S. Constitution. Court agrees:

- Software publication is within constitutional “freedom of speech”.
- NSA’s export regulations are an unconstitutional censorship regime.
- NSA’s revised export regulations are also unconstitutional.

NSA appeals, loses again. Meanwhile: other lawsuits; political pressure; “doors are open”.
U.S. crypto censorship mostly disappears.

Hiring many mathematicians

NSA is the “largest employer of mathematicians in the world”.

Hiring many mathematicians

NSA is the “largest employer of mathematicians in the world”.

IDA hires (e.g.) Coppersmith, whose pre-IDA papers earned the 2022 Levchin Prize for “foundational innovations in cryptanalysis”.

Hiring many mathematicians

NSA is the “largest employer of mathematicians in the world”.

IDA hires (e.g.) Coppersmith, whose pre-IDA papers earned the 2022 Levchin Prize for “foundational innovations in cryptanalysis”.

NSA establishes a “sabbatical program to allow mathematicians to visit us while retaining their academic affiliation”,
and a summer program for students.

Lifetime post-employment secrecy obligation is upheld by the courts.

Post-quantum cryptography

Often a used-car salesman secretly knows
that the car is defective—a “lemon”.
A buyer finds out only after purchasing.

Economists call this a “lemon market”.

Post-quantum cryptography

Often a used-car salesman secretly knows
that the car is defective—a “lemon”.
A buyer finds out only after purchasing.

Economists call this a “lemon market”.

For comparison, post-quantum crypto:

- There are many lemons.

Post-quantum cryptography

Often a used-car salesman secretly knows
that the car is defective—a “lemon”.
A buyer finds out only after purchasing.

Economists call this a “lemon market”.

For comparison, post-quantum crypto:

- There are many lemons.
- In most cases, buyers don’t know that they’re buying lemons.

Post-quantum cryptography

Often a used-car salesman secretly knows
that the car is defective—a “lemon”.
A buyer finds out only after purchasing.

Economists call this a “lemon market”.

For comparison, post-quantum crypto:

- There are many lemons.
- In most cases, buyers don’t know that they’re buying lemons.
- In most cases, sellers don’t know that they’re selling lemons!

Post-quantum cryptography

Often a used-car salesman secretly knows that the car is defective—a “lemon”.
A buyer finds out only after purchasing.

Economists call this a “lemon market”.

For comparison, post-quantum crypto:

- There are many lemons.
- In most cases, buyers don’t know that they’re buying lemons.
- In most cases, sellers don’t know that they’re selling lemons!

Different incentives from a lemon market.

Examples of post-quantum lemons

NIST advertises its pq competition as having 69 submissions from 278 submitters.

17 submissions now known to be breakable on a laptop: CFPKM, Compact LWE, DME, Edon-K, Giophantus, Guess Again, HK17, LUOV-7, pqsigRM, qTESLA-s, RaCOSS, Rainbow-1, Round2, RVB, SIKE, SRTPI, WalnutDSA. Some of these were high-profile submissions from experienced teams.

Make sure to wear your seatbelt

Chrome and Cloudflare jointly ran a big post-quantum experiment in 2019 with two pq proposals: NTRU and SIKE.

Critical: this was a “hybrid” experiment. User data was encrypted with the pq proposal *and* an established system (X25519), so security problems in the pq proposal wouldn’t leave users with *less* security.

We now know SIKE was providing no security!

Make sure to wear your seatbelt

Chrome and Cloudflare jointly ran a big post-quantum experiment in 2019 with two pq proposals: NTRU and SIKE.

Critical: this was a “hybrid” experiment. User data was encrypted with the pq proposal *and* an established system (X25519), so security problems in the pq proposal wouldn’t leave users with *less* security.

We now know SIKE was providing no security!

OpenSSH deployed NTRU Prime + X25519.

Unstable security evaluations

For almost all submissions, public attack algorithms in 2022 are much faster than public attack algorithms in 2017.

Lattice attacks: 2021.10 survey listed 17 new algorithms in 2018–2021. There have been several new attack algorithms in 2022.

Unstable security evaluations

For almost all submissions, public attack algorithms in 2022 are much faster than public attack algorithms in 2017.

Lattice attacks: 2021.10 survey listed 17 new algorithms in 2018–2021. There have been several new attack algorithms in 2022.

Surely NSA knows how to break some of the publicly unbroken submissions.

Unstable security evaluations

For almost all submissions, public attack algorithms in 2022 are much faster than public attack algorithms in 2017.

Lattice attacks: 2021.10 survey listed 17 new algorithms in 2018–2021. There have been several new attack algorithms in 2022.

Surely NSA knows how to break some of the publicly unbroken submissions. Has NSA influenced NIST to select those?

Unstable security evaluations

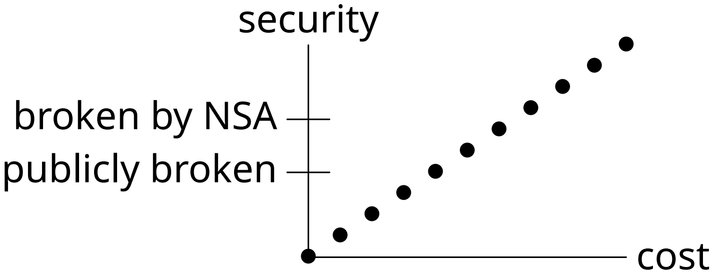
For almost all submissions, public attack algorithms in 2022 are much faster than public attack algorithms in 2017.

Lattice attacks: 2021.10 survey listed 17 new algorithms in 2018–2021. There have been several new attack algorithms in 2022.

Surely NSA knows how to break some of the publicly unbroken submissions. Has NSA influenced NIST to select those? (Hopefully NSA can’t break *all* submissions!)

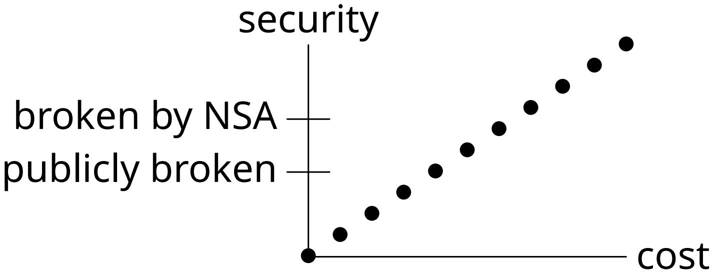
Maybe no influence was needed

Simple model of security vs. cost:



Maybe no influence was needed

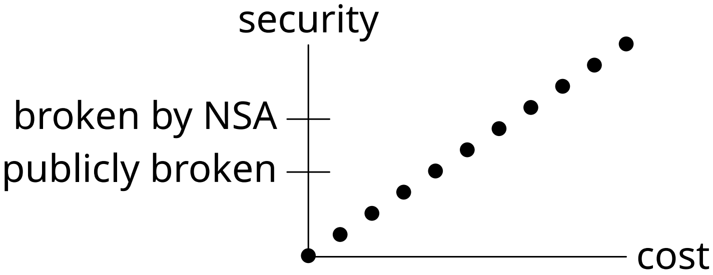
Simple model of security vs. cost:



Now what happens if NIST selects
the fastest publicly unbroken submission?

Maybe no influence was needed

Simple model of security vs. cost:



Now what happens if NIST selects the fastest publicly unbroken submission?
(Hopefully reality isn’t this simple!)

What NIST says

$<$2020: No admission that NSA was involved.

2020.07: I point out transparency failures.

What NIST says

$<$2020: No admission that NSA was involved.

2020.07: I point out transparency failures.

2020.09: NIST says “The feedback received (from the NSA) did not change any of our decisions and did not substantively change our 2nd Round Report” etc.

What NIST says

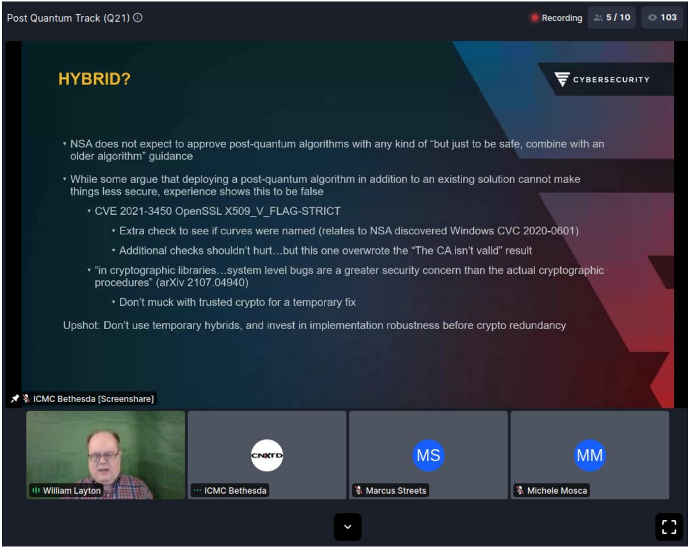
$<$2020: No admission that NSA was involved.

2020.07: I point out transparency failures.

2020.09: NIST says “The feedback received (from the NSA) did not change any of our decisions and did not substantively change our 2nd Round Report” etc.

2020.10: NIST says “We operate transparently. We’ve shown all our work and ensured that there’s traceability” etc.

NSA says: we will not buy seatbelts



HYBRID?

- NSA does not expect to approve post-quantum algorithms with any kind of "but just to be safe, combine with an older algorithm" guidance
- While some argue that deploying a post-quantum algorithm in addition to an existing solution cannot make things less secure, experience shows this to be false
  - CVE 2021-3450 OpenSSL X509_V_FLAG-STRICT
    - Extra check to see if curves were named (relates to NSA discovered Windows CVC 2020-0601)
    - Additional checks shouldn't hurt…but this one overwrote the "The CA isn't valid" result
  - "in cryptographic libraries…system level bugs are a greater security concern than the actual cryptographic procedures" (arXiv 2107.04940)
    - Don't muck with trusted crypto for a temporary fix

Upshot: Don't use temporary hybrids, and invest in implementation robustness before crypto redundancy

NSA also says: delay pq deployment

2021.08: “The intention is to update CNSA to remove quantum-vulnerable algorithms and replace them with a subset of the quantum-resistant algorithms selected by NIST . . . NSA is waiting for the NIST process to be completed and for standards to be published. . . . NSS customers are reminded that NSA does not recommend and policy does not allow implementing or using unapproved, non-standard or experimental cryptographic algorithms. The field of quantum-resistant cryptography is no exception.”

NIST says: delay pq deployment

2021.07 NIST talk: “Don’t let folks start to buy and implement unstandard, unknown, potentially unsecured implementations before we as a general community have agreed upon standardization.”

So NSA+NIST are *objecting* to the real-world post-quantum deployment in, e.g., OpenSSH.

NIST says: delay pq deployment

2021.07 NIST talk: “Don’t let folks start to buy and implement unstandard, unknown, potentially unsecured implementations before we as a general community have agreed upon standardization.”

So NSA+NIST are *objecting* to the real-world post-quantum deployment in, e.g., OpenSSH.

2013 Forbes article says “Leaked NSA doc says it can collect and keep your encrypted data as long as it takes to crack it”; certainly NSA is continuing to collect ciphertexts today.

Mommy, mommy, are we there yet?

NIST delayed announcement half a year working on patent buyouts for Kyber, instead of selecting unpatented NTRU in 2021.

Mommy, mommy, are we there yet?

NIST delayed announcement half a year working on patent buyouts for Kyber, instead of selecting unpatented NTRU in 2021.

2022.07: NIST selected Kyber, but said

- “If the agreements are not executed by the end of 2022, NIST may consider selecting NTRU instead of Kyber” and
- NIST wants input on which “specific parameter sets to include” in the standard; could still make changes.

Maybe a draft standard will be issued in 2023.

2020s: my second lawsuit

2020.09: I start filing FOIA requests. NIST's answers are generally very slow, obviously incomplete.

2022.03: I ask for the full NISTPQC records.

2022.08: I file a FOIA lawsuit.

2022.09: NIST starts delivering some records.

2022.10: NIST says a search found "roughly 514,000 potentially responsive records" but "some or many" may be duplicates. They expect to finish processing by end of 2023.