The Estonian ID-incident from the View-Point of Systems' Engineers and Cryptographers

Ahto Buldas ahto.buldas@ttu.ee

Nov 6, 2017

History

1883: Kerckhoffs's principle

1948: Information Theory (Shannon)

1949: Theory of Secure Communication (Shannon)

Open academic research in cryptography began only in 1970s

1975: Data Encryption Standard (DES)

1976: Diffie-Hellman key exchange protocol

1977: Rivest-Shamir-Adlemann (RSA) asymmetric cryptosystem

Kerchoffs's Principle and Transparent Systems

Auguste Kerckhoffs wrote down the principles of crypto that are followed since today:

- Cryptography should remain secure, if the adversary knows how it works.
- Secrecy of keys must be sufficient to preserve security.

Does not teach how security is measured

Shannon's Theory

Measure of information through probability

Security measured as Entropy

Assumes adversaries with unlimited computational resources

Implications:

Secure system must use very large secret keys

Almost all today's systems are totally insecure

Good theory but very little has been achieved in practice

Example: The entropy of ID-card's private key is zero whenever the public key is known

Modern Cryptography

Assumes adversaries with limited computational resources

Security measured as Complexity of certain attacks

A scheme is S-secure, if any t-time adversary succeeds with probability at most t/S

Implications:

Enables a large variety of cryptographic applications

Measuring security is incomprehensibly complex

None of today's systems have been proved secure

Almost all security proofs in modern cryptography are *relative* and assume hardness of combinatorial problems

Practical Conclusions

Designing and analysing the quality of cryptographic applications is challenging

If a system is built from components, then one has to

- Write down the *requirements* to components
- *Measure* a produced componet to see if it fulfills the requirements

RSA

Invented by Rivest, Shamir and Adleman in 1977

Private key: prime numbers p, q; and exponent d

Public key: modulus $N = pq$ and exponent e

$$ed \mod (p-1)(q-1) = 1 \ .$$

Given a message M:

- *Encryption*: $C = M^e \mod N$
- *Decryption*: $C^d \mod N = M^{ed} \mod N = M$

Private Key Generation

- A large random number r is generated
- Two prime numbers p, q are selected based on r
- Exponent d is computed:

$$d \leftarrow e^{-1} \mod (p-1)(q-1)$$

Secret key is a tuple: $\langle p, q, d \rangle$

In-Device Private Key Generation

Keys are generated inside smart-cards.

Pros: Improved trust model, compared to other generation options

Cons: Slow due to the small computational power

Current Practice in Prime Number Generation

- *Random candidate* p is chosen
- *Trial division*: It is ensured that p is not divisible by any members of a fixed set Π of small prime numbers
- *Exponential tests*, like the Fermat' test is applied:

$$a^{p-1} \mod p = 1$$

for a random $a \leftarrow \{2, 3, \ldots, p-1\}$

The density of n-bit primes is approximately $\frac{1}{n}$.

Division is thousands of times faster than exponentiation.

Trial division eliminates bad candidates fast. Trial division diminishes the average number of exponential tests.

Fast-Prime Methods

Chooses candidates in a way that trial division is not needed.

Choose a first candidate a_0 so that $\gcd(a_0, M) = 1$, where M is the product of all small primes in Π.

Choose the next candidates in the form $a_0 + kM$.

Pros: Faster generation of prime numbers

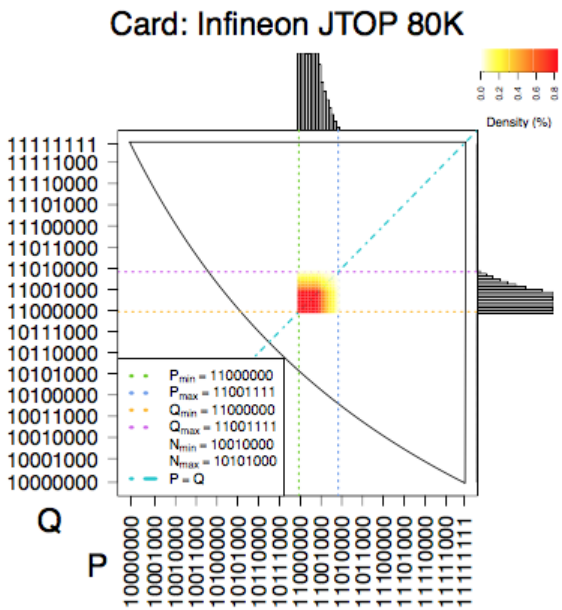
Cons: Lower entropy of prime numbers

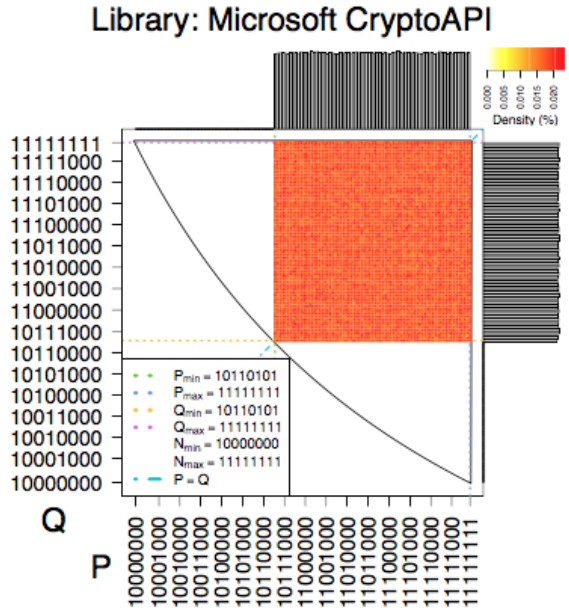
Output Anomalies of Prime Generators

The paper:

"The Million-Key Question – Investigating the Origins of RSA Public Keys" by Svenda, Nemec, Sekan, Kvasnovsky, Formanek, Komarek, and Matyas

analyses the output of several smart-card prime generators. Anomalies in the Infineon's output distribution were discovered.





Formula for the Infineon Primes

The paper:

"The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli." by Nemec, Sys, Svenda, Klinec, and Matyas.

revealed that the Infineon chip's prime numbers are in the form:

$$p = 65537^a \mod M + kM \ ,$$

where M is constant and the same for all chips.

For 2048-bit modulus N, M is the product of the first 126 primes.

All public moduli N satisfy $(65537^c - N) \bmod M = 0$ for some c.

Such c is found in microseconds by the Pohlig-Hellman algorithm

This test was disclosed by the authors in spring 2017, and reached Estonia in August 2017.

Coppersmith's Attack

Theorem (Coppersmith 1996)

Having $n/4$ most significant bits of p, any n-bit RSA modulus $N = pq$ can be efficiently factored

Naive Attack

Try all $\mathrm{ord}_M(65537)$ possible a-s and try to find k by Coppersmith's attack

Here, $\mathrm{ord}_M(65537)$ is the order of 65537 in the multiplicative group $\mathbb{Z}_M^*$

Naive search is infeasible: the number of a-s to examine is 2^{254}.

Making the Naive Attack Efficient

Main idea: Use a divisor M' of M, such that $\mathrm{ord}_{M'}(65537)$ is feasible, but still the number of bits in M' is larger than $2048/4$ (necessary for the Coppersmith's attack).

Then, the prime numbers are still expressible in the form:

$$p = 65537^{a'} \mod M' + k'M'$$

Authors found optimal M' in terms of the overall attack time by brute force search combined with greedy heuristics.

Impact of the Attack

By using optimal M', the number of possible a-s is 2^{34} for 2048-bit RSA modulus

k is found in 200 ms on a desktop computer by using Coppersmith's algorithm

The total costs by key estimated by authors:

- *30000 EUR* in Amazon cloud
- *1000 EUR* for electricity, without taking hardware into account

Conclusions

Certified≠secure: Though the Infineon chip was certified by Common Criteria, it does not mean it is secure against unknown attacks

Vulnerabilities in soft- and hardware are inevitable

IT-Systems design/management must take potential unknown vulnerabilities into account