Introduction to asymmetric crypto

Ideas for the rest of the fall

Martin Strand
Forsvarets forskningsinstitutt

7 October 2020

Today’s goal

Introduce the central ideas you will explore the rest of the term

Today's goal

Introduce the central ideas you will explore the rest of the term

Question

What is the commonality of everything you've seen thus far?

Today's goal

Introduce the central ideas you will explore the rest of the term

Question

What is the commonality of everything you've seen thus far? How can we get there?

Preliminaries: Groups

Definition (Group)

An group $(G, \cdot)$ consists of a set G and a binary operation $\cdot$ on G such that the following axioms hold:

1. (Associativity) $a(bc) = (ab)c$ for all $a, b, c \in G$.
2. (Identity element) There exists $1 \in G$ such that $1a = a$ for all $a \in G$.
3. (Inverses) For every $a \in G$ there exists an $b \in G$ such that $ba = 1$. Write $b = a^{-1}$.

Definition (Subgroup)

Let $(G, \cdot)$ be a group, and let $H \subseteq G$. If H is closed under $\cdot$, then H is a subgroup of G, written $H < G$.

Definition (Abelian group)

The group G is abelian if $\cdot$ is commutative, i.e. $ab = ba$ for all $a, b \in G$.

Preliminaries: Cyclic groups

Definition (Order of a group)

Let G be a group. The order of G is the cardinality of G. (I.e., the number of elements.)

Definition (Order of element)

Let G be a group and $a \in G$. If there exists a least positive integer m such that $a^m = 1$, then m is called the order of a, written $o(a)$. If no such integer exists, then a is said to be of infinite order.

Definition (Cyclic group)

Let $g \in G$ and set $G' = \{g^i \mid i \in \mathbb{Z}\}$. Then G' is the subgroup of G generated by g, denoted $\langle g \rangle$.

Note: $|\langle g \rangle| = o(g)$

Preliminaries: Cosets

Definition (Cosets)

Let H be a subgroup of G. For $g \in G$, the left cosets of H in G are the sets

$$gH = \{gh \mid h \in H\}$$

The set of all left cosets of H in G is written G/H.

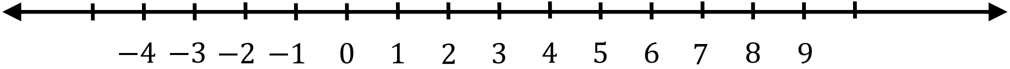
Let $\sim$ be the equivalence relation defined by $a \sim b$ if and only if $aH = bH$. Hence G/H is a partition of G. Under $\sim$, G/H becomes a group.

Example

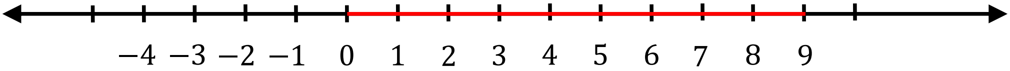
Let $G = (\mathbb{Z}, +)$ be a group with the subgroup $\langle n \rangle = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$. Then all cosets of G are

$$\begin{aligned}
\langle n \rangle &= \{\ldots, -2n, -n, 0, n, 2n, \ldots\} \\
1 + \langle n \rangle &= \{\ldots, 1 - 2n, 1 - n, 1, 1 + n, 1 + 2n, \ldots\} \\
2 + \langle n \rangle &= \{\ldots, 2 - 2n, 2 - n, 2, 2 + n, 2 + 2n, \ldots\} \\
&\vdots \\
(n-1) + \langle n \rangle &= \{\ldots, (n-1) - 2n, (n-1) - n, n - 1, (n-1) + n, (n-1) + 2n, \ldots\}
\end{aligned}$$

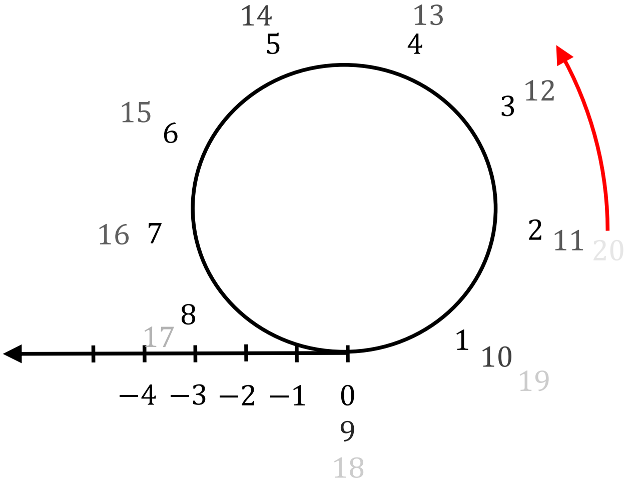
Modular arithmetic



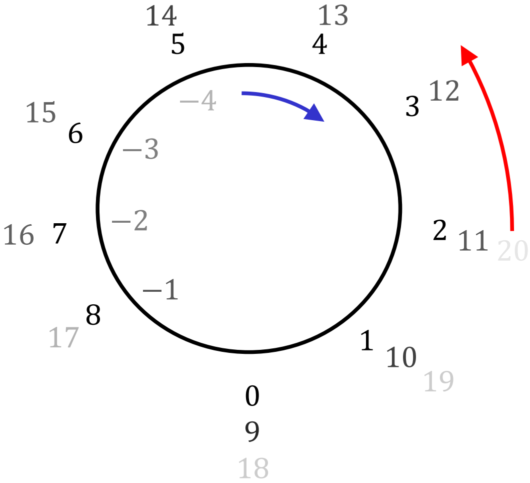
Modular arithmetic



Modular arithmetic



Modular arithmetic



Example

The set

$$\mathbb{Z}/\langle n \rangle = \{\langle n \rangle, 1 + \langle n \rangle, 2 + \langle n \rangle, \ldots, (n-1) + \langle n \rangle\}$$

is a group and is isomorphic (“essentially the same”) to the group $\{0, \ldots, n-1\}$ under addition modulo n, and we write $\mathbb{Z}_n$.

Theorem (Lagrange)

Let G be a finite group. Then the order of any subgroup of G divides the order of G.

Corollary

Let G be a group of finite order n. Then for every $a \in G$, $o(a)|n$, and, hence, $a^n = 1$.

Corollary (Fermat's little theorem)

Let p be a prime number. Then for any $a \in \mathbb{Z}$,

$$a^p \equiv a \pmod{p}.$$

If a is not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Setting the stage

- Let n be a positive integer, and consider the set $\mathbb{Z}_n$.
- Is this a group under multiplication modulo n?

Setting the stage

- Let n be a positive integer, and consider the set $\mathbb{Z}_n - \{0\}$.
- Is this a group under multiplication modulo n?

Setting the stage

- Let p be a prime, and consider the set $\mathbb{Z}_p - \{0\}$.
- Is this a group under multiplication modulo p?

Setting the stage

- Let p be a prime, and consider the set $\mathbb{Z}_p - \{0\}$.
- Is this a group under multiplication modulo p?
- We call this group $\mathbb{Z}_p^*$, and it has $p - 1$ elements.
- Take some $g \in \mathbb{Z}_p^*$ and consider $G = \langle g \rangle$.

Example in Python

```
p = some_prime(bitlength)
g = 2
h = pow(g, a, p)
```

Diffie-Hellman key exchange

Martin		you
Random $0 < a < p - 1$		
Set $A = g^a$	$\xrightarrow{A}$	Random $0 < b < p - 1$
	$\xleftarrow{B}$	Set $B = g^b$
Set $C_1 = B^a$		Set $C_2 = A^b$

Completeness

Claim

We have $C_1 = C_2$.

$$\begin{aligned} C_1 &= B^a = \left(g^b\right)^a \\ &= g^{ba} = g^{ab} \\ &= (g^a)^b = A^b \\ &= C_2 \end{aligned}$$

Let’s try

```
p = 107
g = 5
b = pick_one_at_random
B = pow(g, b, p)

A = receive_from_Martin
C = pow(A, b, p)
```

Is the value private to us?

Definition (Computational Diffie-Hellman Problem (CDH))

Given $(g, g^a, g^b) \in G \times G \times G$, compute $g^{ab} \in G$

Is the value private to us?

Definition (Computational Diffie-Hellman Problem (CDH))

Given $(g, g^a, g^b) \in G \times G \times G$, compute $g^{ab} \in G$

Definition (Decisional Diffie-Hellman Problem (DDH))

Distinguish the following two tuples:

$$\begin{aligned} (g, g^a, g^b, g^{ab}) &\in G^4; \quad a, b \text{ random} \\ (g, g^a, g^b, g^c) &\in G^4; \quad a, b, c \text{ random} \end{aligned}$$

How can it be secure?

Let $p - 1 = n = n_1^{e_1} n_2^{e_2} \cdots n_k^{e_k}$, and assume g has maximal order.

- n must be exponentially large
  - — Exhaustive search will find a in time $O(n)$
  - — Hence lower bound on $\log_2(n)$
- *Baby-step, giant step* (BSGS) or *Pollard's rho* algotithms have running time $O(\sqrt{n})$
- The *Pohlig-Hellman* algorithm and the Chinese Remainder Theorem divides the problem into subproblems for each $n_i, n_i^2, \ldots n_i^{e_i}$
  - — Let $n' = \max\{n_1, \ldots n_k\}$. Pohlig-Hellman with Pollard's rho or BSGS runs in $O(e' \sqrt(n')) \approx O(\exp(1/2 \ln(n')))$
  - — Hence lower bound on the square root of the largest prime factor of $p - 1$ ($\frac{p-1}{2}$ should be prime)

How can it be secure?

Let $p - 1 = n = n_1^{e_1} n_2^{e_2} \cdots n_k^{e_k}$, and assume g has maximal order.

- n must be exponentially large
  - — Exhaustive search will find a in time $O(n)$
  - — Hence lower bound on $\log_2(n)$
- *Baby-step, giant step* (BSGS) or *Pollard's rho* algotithms have running time $O(\sqrt{n})$
- The *Pohlig-Hellman* algorithm and the Chinese Remainder Theorem divides the problem into subproblems for each $n_i, n_i^2, \ldots n_i^{e_i}$
  - — Let $n' = \max\{n_1, \ldots n_k\}$. Pohlig-Hellman with Pollard's rho or BSGS runs in $O(e' \sqrt(n')) \approx O(\exp(1/2 \ln(n')))$
  - — Hence lower bound on the square root of the largest prime factor of $p - 1$ ($\frac{p-1}{2}$ should be prime)
- (Exploiting the additive structure as well,) Index Calculus with complexity

$$\exp\left(\sqrt[3]{\frac{64}{9}\ln(n')(\ln\ln(n'))^2}\right)$$

Number of atoms in the universe

100 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000 000 000 000 000 000 000 000 000 000

Number of unique chess games

```
1 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
  000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
  000 000 000 000 000 000 000 000
```

A suitable prime for Diffie-Hellman

```
17 371 633 710 861 526 985 402 756 155 605 996 322 196 257 048 455
   675 141 997 211 607 897 588 436 880 112 664 345 732 402 516 434
   975 116 670 023 472 796 825 233 643 612 395 266 186 808 119 984
   996 372 379 602 426 678 900 493 286 192 039 475 551 678 848 776
   585 415 169 949 664 415 820 483 514 690 301 509 982 058 398 659
   940 050 744 425 005 234 342 360 377 140 221 362 953 519 273 046
   483 446 364 930 471 865 451 176 965 825 059 235 201 349 014 188
   384 323 322 347 988 836 585 004 216 878 741 293 400 993 565 478
   114 200 002 489 905 246 623 078 674 988 568 740 682 222 428 856
   692 842 421 774 076 905 917 061 448 967 466 083 362 856 797 534
   215 180 379 822 041 036 186 832 388 654 983 120 685 889 564 412
   266 789 511 781 064 026 694 452 185 724 178 282 543 463 162 021
   793 730 933 403 449 281 865 751 197 897 543 205 563
```

Improved solution: Elliptic curves

(But I've got to leave some fun for Håkon, right?) Note: At this point I drew the group law on the blackboard. Wikipedia has a nice picture of the process, `https://en.wikipedia.org/wiki/Elliptic_curve`.

Representation means something

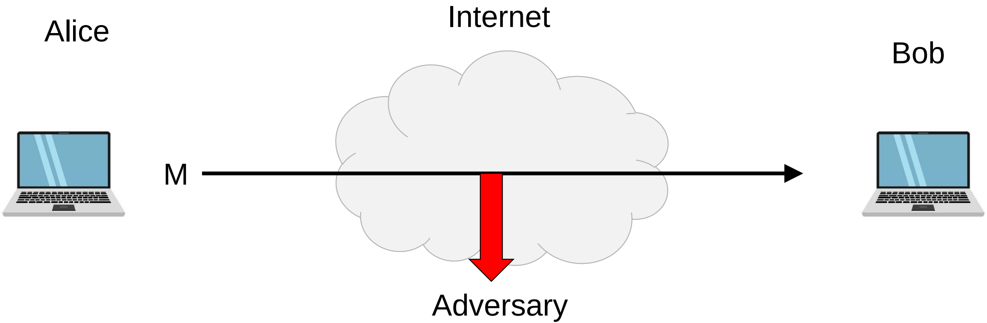
Every finite cyclic group is isomorphic to $(\mathbb{Z}_n, +)$ for some n.

- Diffie-Hellman over $(\mathbb{Z}_n, +)$: :-(
- Diffie-Hellman over $(\mathbb{Z}^*_{2q+1}, \cdot)$: :-|
- Diffie-Hellman over $H < (\mathbb{Z}^*_{2q+1}, \cdot)$: :-)
- Diffie-Hellman over elliptic curves: :-D

Dlog

If you can compute the isomorphism, then you can break the Diffie-Hellman key exchange. This is the *discrete logarithm problem*.

What is cryptography?



Alice

Internet

Bob

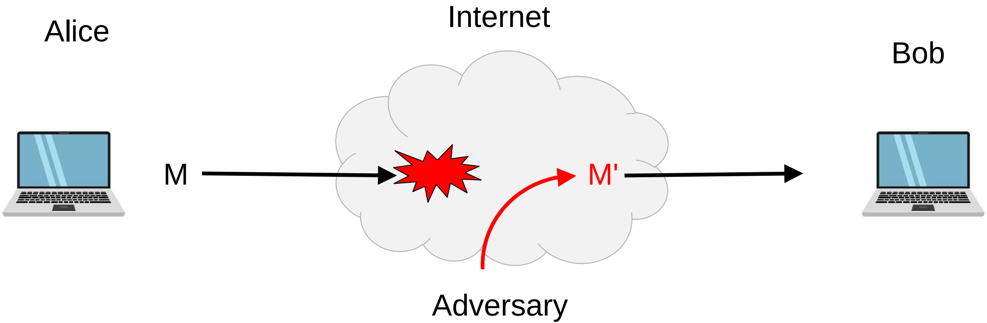
M

Adversary

Security goals:

- **Data privacy:** adversary should not be able to read message M

What is cryptography?



Security goals:

- **Data privacy:** adversary should not be able to read message M
- **Data integrity:** adversary should not be able to modify message M
- **Data authenticity:** message M really originated from Alice

My keys

Public-key crypto in a nutshell

Private: Can open the box
RSA: *d*

Public: Can lock the box
RSA: *e*

My keys

Public-key crypto in a nutshell

Private: Can open the box
RSA: *d*

Public: Can lock the box
RSA: *e*

What happens if we switch the keys?

Distracted-me-keys

Signatures in a nutshell

Public: Can open the box

Private: Can lock the box

More algebra

Definition (Euler totient function)

Let n be a positive integer. Define $\varphi(n)$ as the number of integers between 1 and n with no common divisors with n.

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

More algebra

Definition (Euler totient function)

Let n be a positive integer. Define $\varphi(n)$ as the number of integers between 1 and n with no common divisors with n.

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

Theorem (Euler)

Let n and a be integers with $\gcd(a, n) = 1$*. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Rivest-Shamir-Adleman

Let p, q be primes, and set $n = pq$. Consider the multiplicative group $\mathbb{Z}_n^*$.

Rivest-Shamir-Adleman

Let p, q be primes, and set $n = pq$. Consider the multiplicative group $\mathbb{Z}_n^*$. Choose integers e, d such that $ed \equiv 1 \pmod{\varphi(n)}$. Keep d private and publish (e, n).

Rivest-Shamir-Adleman

Let p, q be primes, and set $n = pq$. Consider the multiplicative group $\mathbb{Z}_n^*$. Choose integers e, d such that $ed \equiv 1 \pmod{\varphi(n)}$. Keep d private and publish (e, n).

Encrypt(m) Output $c \leftarrow m^e \pmod{n}$

Decrypt(c) Output $m \leftarrow c^d \pmod{n}$

Rivest-Shamir-Adleman

Let p, q be primes, and set $n = pq$. Consider the multiplicative group $\mathbb{Z}_n^*$. Choose integers e, d such that $ed \equiv 1 \pmod{\varphi(n)}$. Keep d private and publish (e, n).

Encrypt(m) Output $c \leftarrow m^e \pmod{n}$

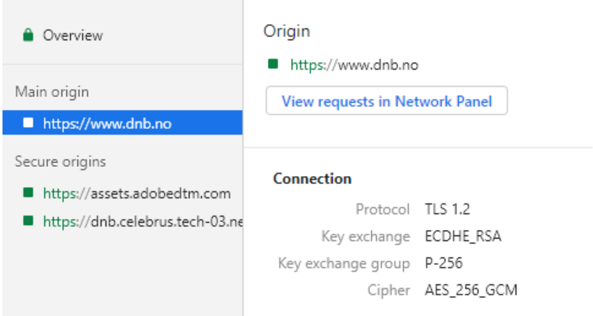
Decrypt(c) Output $m \leftarrow c^d \pmod{n}$

Correctness

$$c^d = (m^e)^d = m^{ed} = m^{1+\ell\varphi(n)} = m \cdot \left(m^{\varphi(n)}\right)^\ell \equiv m \pmod{n}$$

Some questions to consider

- Is this IND-CPA?
- Is this IND-CCA?



Overview
Main origin
https://www.dnb.no
Secure origins
https://assets.adobedtm.com
https://dnb.celebrus.tech-03.ne
View requests in Network Panel

Origin

🟩 https://www.dnb.no

Connection

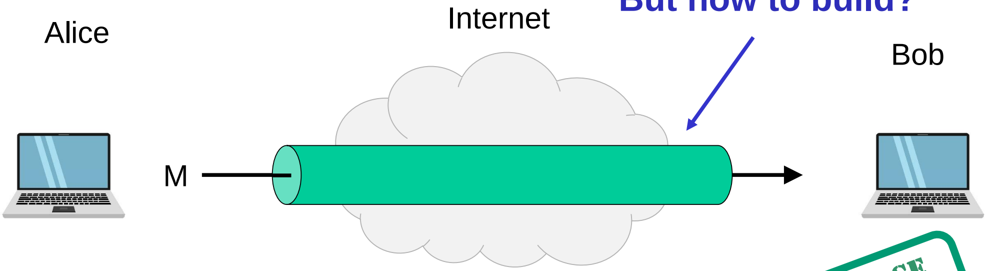
Protocol TLS 1.2

Key exchange ECDHE_RSA

Key exchange group P-256

Cipher AES_256_GCM

Ideal solution: secure channels



But how to build?

Adversary

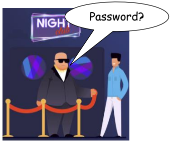
COURSE DONE!

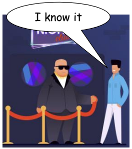
Security goals:

- **Data privacy:** adversary should not be able to read message M ✓
- **Data integrity:** adversary should not be able to modify message M ✓
- **Data authenticity:** message M really originated from Alice ✓

Much more to cryptography

- Zero-knowledge proofs



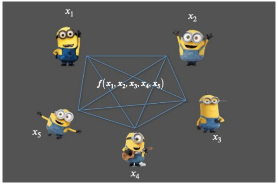


NIGHT club
Welcome!

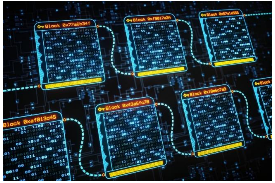
- Fully-homomorphic encryption

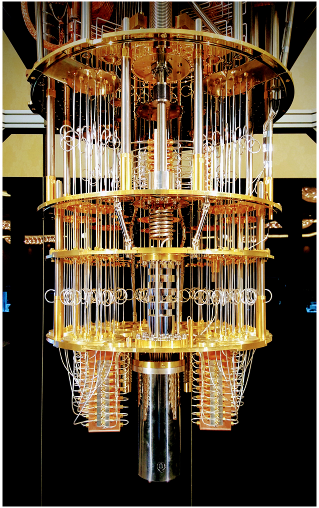
$$Enc(K, M_1 + M_2) = Enc(K, M_1) + Enc(K, M_2)$$

- Multi-party computation

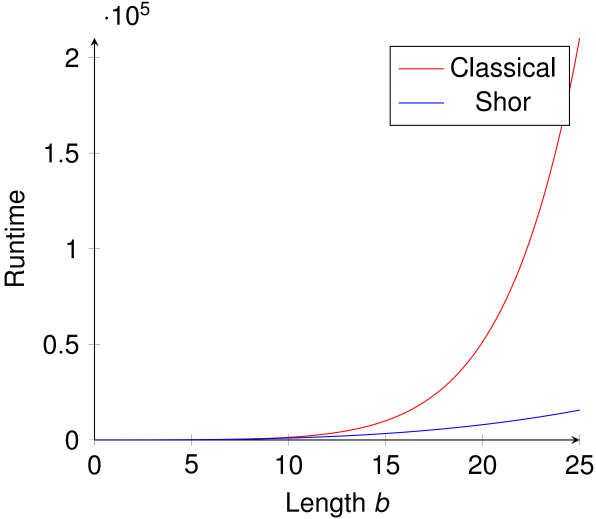


- Blockchain





Shor's algoritme vs. dlog and factorisation



Consequences for crypto

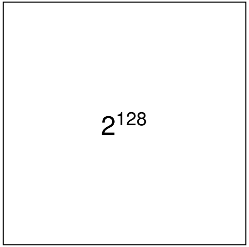
- RSA
- ElGamal
- AES
- Diffie-Hellman
- SHA-2
- SHA-3
- Elliptic curve Diffie-Hellman

Consequences for crypto

- ~~RSA~~
- ~~ElGamal~~
- AES
- ~~Diffie-Hellman~~
- SHA-2
- SHA-3
- ~~Elliptic curve Diffie-Hellman~~

Grover's algorithm

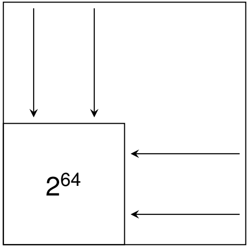
(In theory)



2^{128}

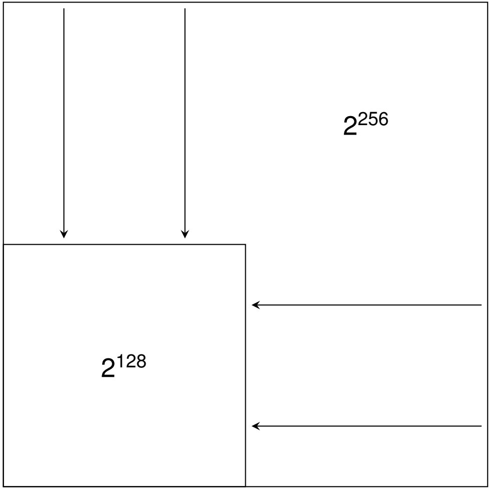
Grover's algorithm

(In theory)

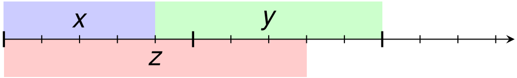


Grover's algorithm

(In theory)



Quantum computers are coming (?)



Theorem (Mosca)

If $x + y > z$, be anxious.

Solutions

- NIST Post-Quantum Cryptography Standardization
- 69 initial candidates (2017) – 7 (8) finalists (alternates) remaining:

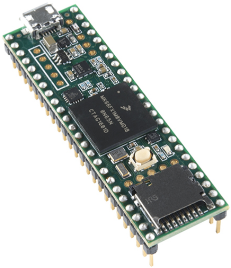
Key encapsulation

- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

Signature

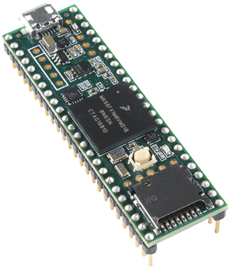
- FALCON
- CRYSTALS-DILITHIUM
- Rainbow

This summer's project



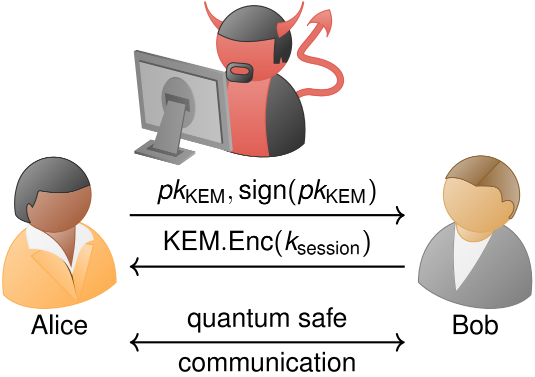
- Run the NIST-candidates on a very small and cheap processor often used on devices.
- Teensy 3.6 with ARM Cortex M4 processor (32 bit, 180 MHz), 256 kB memory.

This summer’s project



- Run the NIST-candidates on a very small and cheap processor often used on devices.
- Teensy 3.6 with ARM Cortex M4 processor (32 bit, 180 MHz), 256 kB memory.
- 1995 performance coupled with 1985 memory.

Our demo protocol (simplified)



Alice

$pk_{\text{KEM}}, \text{sign}(pk_{\text{KEM}})$ →

← $\text{KEM.Enc}(k_{\text{session}})$

quantum safe ↔ communication

Bob

Some selected results

Sizes in bytes

System	Public key	Private key	Ciphertext
KYBER	1184	2400	1088
NTRU	1230	1590	1230
SABER	992	2304	1088
FrodoKEM	15632	31296	15744
SIKE	462	524	486

Some selected results

Times in milliseconds

System	Key generation	Encryption	Decryption
KYBER	5	6	6
NTRU	1462	7	10
SABER	6	8	9
FrodoKEM	1005	1009	1000
SIKE	673	1234	1241

Want more?

TEK5550

Midterm test

- Mandatory
- Pass/fail grading: Passing grade required to sit the exam
- Deadline 20 October
- Submit in Canvas
- Individual; no collaboration allowed

https://www.uio.no/studier/emner/matnat/its/TEK4500/h20/Messages/next-week-tuesday-6-october-midterm-assi.html