The RSA Algorithm

Private-key cryptosystems:
- Alice and Bob agree on the key before the communication
- all cryptosystems we discussed so far
- also called: symmetric-key cryptosystems

Public-key cryptosystems (Chapter 6):
- what to do if Alice and Bob do not secretly meet in advance?
- the encryption key is public:
  - encryption function is easy to compute and hard to invert; a so-called one-way function
  - what else do we need from the encryption function? Bob needs to be able to invert the one-way function.
The RSA Algorithm

Remarks:
- we do not know if one-way functions exist...
- we work with functions that are believed to be one-way

- a one-way function that is easy to invert if one has a corresponding private key (a trapdoor) is called a trapdoor one-way function
The RSA Algorithm

Public-key cryptography:
- Diffie-Helman, 1976 (it was documented earlier in classified documents)
- Rivest-Shamir-Adleman, 1977: The RSA Cryptosystem

- never give perfect secrecy - why not?

Note:
- public-key cryptosystems usually used to encrypt a private key, not the complete message - why?
The RSA Algorithm

1. Bob chooses secret odd primes $p$ and $q$, computes $n = pq$.
2. Bob chooses $e$ with $\gcd(e, \Phi(n)) = 1$.
3. Bob computes $d = e^{-1} \mod \Phi(n)$.
4. Bob makes $n$ and $e$ public, keeps $p$, $q$, and $d$ private.
5. Alice encrypts $m \in \mathbb{Z}_n$ as $c = m^e \mod n$ and sends $c$ to Bob.
6. Bob decrypts by computing $m = c^d \mod n$.

What is $\Phi(n)$?

Bob can easily compute, but Alice (and Eve) cannot.

$$\Phi(n) = \# \text{coprimes } < n = p \cdot q$$

$$= (p-1)(q-1)$$

$n = 6$:

$$\{1, 2, 3, 4, 5 \}$

$$n - 1 - 6/p - 1 - (n/q - 1) = pq + 1 - q - p$$

$n = 20$:

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 \}$$

$$= pq + 1 - q - p$$
The RSA Algorithm

1. Bob chooses secret odd primes $p$ and $q$, computes $n = pq$.
2. Bob chooses $e$ with $\gcd(e, \Phi(n)) = 1$.
3. Bob computes $d = e^{-1} \mod \Phi(n)$.
4. Bob makes $n$ and $e$ public, keeps $p$, $q$, and $d$ private.
5. Alice encrypts $m \in \mathbb{Z}_n$ as $c = m^e \mod n$ and sends $c$ to Bob.
6. Bob decrypts by computing $m = c^d \mod n$.

What is $\Phi(n)$?

Bob: $p = 3$
$p = 7$
$n = 21$

Alice:

$m = 4$

Bob:

$m^e \mod n = 4^5 \mod 21 = 16 = c$

Bob:

$c^d \mod n = 16^5 \mod 21 = 4$

Alice:

Boxed: Bob selects
Rest: Bob computes

$\Phi(n) = (p-1)(q-1) = 12$

$e = 5$

does not have to be a prime

$m = 805121215$

hello

$m = 805121215$

$c = 805121215$

$e = 5$

The plaintext

$c = 5$ (usually different than $e$)