Public Key Encryption

- One-way function: \( n = p \cdot q \) | \( n \) given, \( p, q = ? \)

- RSA cryptosystem:
  - \( p, q \) prime, \( n = p \cdot q \), \( e \), \( d = e^{-1} \mod (p-1)(q-1) \)
  - public key: \( n, e \)
  - private key: \( d \)
  - encryption: \( C = m^e \mod n \)
  - decryption: \( m = C^d \mod n \)

- One-way function:
  - \( p \) prime, \( a \) \( \equiv \) \( p \) \( \mod p \): \( y = a^x \mod p \) | given \( y \), \( x = ? \)

- Diffie-Hellman key exchange:
  - A: \( n = a^x \mod p \) \( \Rightarrow \) B: \( n = a^y \mod p \)
  - joint key: \( a^{xy} \mod p = a^{xy} \mod p \)

- One-way function:
  - \( p, q \) prime, \( n = p \cdot q \): \( y = x^2 \mod n \) | given \( y \), \( x = ? \)

- Rabin cryptosystem:
Prop. 9.2. $p > 2$ prime.
$\begin{align*}
c \text{ is } QR \mod p & \iff c^{(p-1)/2} \equiv 1 \pmod{p} \\
\end{align*}$

Prop. 9.3. $p$ prime, $p \equiv 3 \pmod{4}$, i.e., $p = 4k + 1$, $c \text{ is } QR \mod p$. Then
$x^2 \equiv c \pmod{p}$ has the only solutions $x_{1,2} = \pm c^{(p-1)/2} \pmod{p}$.

Remark: For $p \equiv 1 \pmod{4}$ there is no known efficient deterministic alg. for solving $x^2 \equiv c \pmod{p}$. However, there is an efficient probabilistic algorithm.

Prop. 9.4. Let $p \neq q$ prime, $n = p \cdot q$.
Compute by the extended Euclidean alg $s, t \in \mathbb{Z}$ with
$\begin{align*}
sp + tq &= \gcd(p, q) = 1, \\
\frac{s}{p} &= \frac{t}{q} = a
\end{align*}$

Let $a = s$, $b = t$, further $x, y \in \mathbb{Z}$ with
$\begin{align*}
x^2 &\equiv c \pmod{p} \\
y^2 &\equiv c \pmod{q}
\end{align*}$

Then $f = ax + by$ is a solution of $f^2 \equiv c \pmod{n}$. \[\]
Proof. By definition

\[ a = 1 \pmod{p}, \quad b = 0 \pmod{p} \]
\[ a = 0 \pmod{q}, \quad b = 1 \pmod{q} \]

Moreover

\[
(ax+by)^2 \equiv a^2x^2 + 2abxy + b^2y^2 \equiv \begin{cases} x^2 \equiv c \pmod{p} \\ y^2 \equiv c \pmod{q} \end{cases}
\]

By Prop. 8.1 \((ax+by)^2 \equiv c \pmod{u}\). \(\square\)

Remark: There are \(4\) solutions to \(x^2 \equiv c \pmod{u}\), if \(u = p \cdot q\), \(p + q\) prime.

**Rabin Cryptosystem**

(i) \(p + q\) prime, \(n = p \cdot q\), \(p, q \equiv 3 \pmod{4}\)

(ii) Public key: \(n\), private key: \((p, q)\)

(iii) Encryption: \(C = m^2 \pmod{n}\) (message \(m\))

(iv) Decryption: Determine \(x\): \(x^2 \equiv c \pmod{p}\), \(y\): \(y^2 \equiv c \pmod{q}\)

Use Prop. 9.4. \(\overline{OR}\)

\(4\) solutions; choose the one where the last

64 bits are identical, e.g., to the previous set of 64 bits, because they have been replicated before encrypting.
Determine \( f \equiv x \pmod{p} \)
\( f \equiv y \pmod{q} \)

by the Chinese Remainder Theorem.

(4 solutions as well)

\[
\begin{align*}
    f^2 & \equiv x^2 \equiv c \pmod{p} \\
    f^2 & \equiv y^2 \equiv c \pmod{p}
\end{align*}
\]

\( \implies f^2 \equiv c \pmod{pq} \).

Bear in mind: \( m \gg \sqrt{N} \), otherwise a solution is obtained by computing square root over \( \mathbb{R} \).

Remark 9.5. 4 solutions! Identify the right one.

Remark 9.6. (Security of the Rabin system)

a) From Prop 8.1: Breaking "Rabin" is equivalent to factoring.

b) The Rabin system is vulnerable against chosen-ciphertext attack.
\* O/E chooses \( m \) at random, computes \( c = m^2 \mod n. \)
\* \( c \) is deciphered with plaintext \( m' \).
\* With prob. \( \frac{1}{2} : m' \neq \pm m \). In this case
  \[ \gcd(m - m', n) \in \{ p, q \} \] (\( \star \))
  Otherwise, repeat the above.

Hence, never publish a deciphered message
which is not the original one.

Why is (\( \star \)):
\[ x^2 \equiv y^2 \pmod{n}, x \neq \pm y \pmod{n} \]
\[ \Rightarrow \gcd(x-y, n) \in \{ p, q \} \]
Since \( n \mid x^2 - y^2 \Rightarrow n \mid (x-y)(x+y) \)
but \( n \nmid (x-y) \) and \( n \nmid (x+y) \) →

C) Broadcast endagers the Ranam system.
The same message \( m \) is sent to \( K \) receivers \( z_1, \ldots, z_K \),
encrypted by public keys \( n_1, \ldots, n_K \).
\[ c_1 = m^2 \mod n_1 \]
\[ c_k = m^2 \mod n_k \]
(Very likely all
prime factors \( \mu \)
\( n_1, \ldots, n_k \) are
different.)
C/E eavesdrop and solve

\[ x \equiv C_1 \pmod{n_1} \]

\[ x \equiv C_K \pmod{n_K} \]

The Chinese Remainder Theorem yields a solution

\[ x \equiv m^2 \pmod{n_1 \cdots n_K} \]

Since \( m < n_i \) \( \forall i = 1, \ldots, K \), it follows \( m^2 < n_1 \cdots n_K \).

Hence \( x = m^2 \) can be solved for \( m \) over \( \mathbb{R} \).

The same attack can be applied to RSA for small \( e \).
Signature Schemes

Requirements (secure as on conventional signatures)
- verifiable
- forgery-proof
- firmly connected to the document

11.1. El Gamal signature scheme

$h$: hash function

Parameters: $p$: prime, $a$ $\text{PE mod } p$
Select random $x$, $y = a^x \text{ mod } p$
Public key: $(p, a, y)$ Private key: $x$

Signature generation:
Select random $k$ s.t. $k^{-1} \text{ mod } (p-1)$ exists.
$r = a^k \text{ mod } p$
$s = k^{-1} (h(m) - x r) \text{ mod } (p-1)$
Signature for $m$: $(r, s)$
Signature verification:

Verify \( 1 \leq r \leq p-1 \)
\[ v_1 = y^{rs} \mod p \]
\[ v_2 = a \cdot h(m) \mod p \]
\[ v_1 = v_2 \rightarrow \text{accept signature.} \]

Verification works:

\( ks \equiv l(v) - x r \pmod{p-1} \)
\[ \Rightarrow l(v) = x r + ks \pmod{p-1} \]
\[ \Rightarrow x r + ks = l(p-1) + h(m) \text{ for some } l \in \mathbb{Z} \]

Here

\( y^{rs} \equiv a x r k s = a x r + ks \)
\[ = a \cdot l(p-1) + a \cdot h(m) \]
\[ = (a^{p-1}) \cdot a \cdot h(m) = a \cdot h(m) \pmod{p} \]
\[ = l(h(m) \pmod{p}) \text{ (Fermat's)} \]