9 Public key Encryption (ctd.)

9.1 A Side Channel attack against RSA

Recall RSA public-key encryption:

$n = p \cdot q$, $p \neq q$ primes

$d \in \mathbb{Z}^*_{\varphi(n)}$, i.e., $gcd(d, \varphi(n) = (p-1)(q-1)) = 1$

Public key: $(e = d^{-1}, n)$ Private (d, p, q)

Encryption: $c = m^e \mod n$

Decryption: $m = c^d \mod n$

} exponentiation is the most expensive computational part of RSA.

Use the Chinese Remainder Theorem (CRT) to speed decryption.

(i) Compute $m_1 = c^d \mod p$

Since $c^{p-1} \equiv 1 \mod p$, compute $m_1 = c^{d \bmod p-1} \mod p$

(ii) Compute $m_2 = c^{d \bmod q-1} \mod q$

(iii) Determine m such that

$$m \equiv m_1 \mod p$$
$$m \equiv m_2 \mod q$$

Solution: By the extended Euclidean alg (EEA) compute a, b with $a \cdot p + b \cdot q = 1$, i.e., $a \equiv p^{-1} \pmod q$, $b \equiv q^{-1} \pmod p$

(This computation is necessary only once)

With the CRT:

$$m = (a \cdot q \cdot m_1 + b \cdot p \cdot m_2) \mod n$$

By CRT $m \equiv c^d \mod n$ is unique.

This method is approximately 4 times faster as direct computation, since numbers are of approx. half bit length, half the number of squarings are needed for SQM (square-and-multiply) with complexity $O(n^2)$ for squaring/multiplication and it is done twice.

Attack against smartcards with this implementation by random hardware faults causing incorrect values.
By e.g., high temperature, irregular clock frequency or voltage, radiation, magnetism, power drain: cause exactly one false computation.

Available are

m correct deciphering with m_1, m_2 from (i) and (ii)
$\hat{m}$ faulty decryption with error in $\hat{m}_1$ of (i)

$$(m - \hat{m}) = a \cdot q (m_1 - \hat{m}_1) + b \cdot p (m_2 - \hat{m}_2)$$

Assumption $m_1 \not\equiv \hat{m}_1 \bmod p$
$m_2 \equiv \hat{m}_2 \bmod q$

Hence, $m \not\equiv \hat{m} \bmod p$, but $m \equiv \hat{m} \bmod q$

$p \nmid (m - \hat{m})$ $\quad q \mid (m - \hat{m})$

$\Rightarrow m - \hat{m} = l \cdot q \quad l \in \mathbb{Z}, \; |l| < p$

$n = p \cdot q$

$\gcd(m - \hat{m}, n) = q$

9.2 Rabin cryptosystem (Repetition)

Like RSA with $e = 2$, however, $\nexists d : e \cdot d \equiv 1 \pmod{\ell(n)}$
as $gcd(2, \ell(n)) = 2$ ($\ell(n) = (p-1)(q-1)$)

$\Rightarrow$ Deciphering means to calculate square roots modulo n
But computing square roots is no easier than factoring (Chapter 8)

Prop 8.3: $n = p \cdot q$, x non-trivial solution of $x^2 \equiv 1 \pmod{n}$

$\Rightarrow gcd(x+1, n) \in \{p, q\}$

Computing square roots modulo p, q is easy.

Def 9.1 c is called quadratic residue (QR) modulo n, if

$\exists x : x^2 \equiv c \pmod{n}$

Prop 9.2 Euler's criterion

$p > 2$, p Prime: c is QR mod p $\Leftrightarrow$ $c^{(p-1)/2} \equiv 1 \pmod{p}$

No indication on how to get x.

Prop 9.3: p prime, $p \equiv 3 \pmod 4$, i.e., $p = 4k - 1$, $k \in \mathbb{N}$,
c QR mod

$\Rightarrow x^2 \equiv c \pmod{p}$ has the only solutions $x_{1,2} = \pm c^k \bmod p$

Remark: $p \equiv 1 \pmod 4$: no known deterministic alg. to calculate x,
but polynomial time probabilistic alg. are known.

Rabin cryptosystem

(i) $p \neq q$ prime, $p, q \equiv 3 \pmod 4$ $\quad n = p \cdot q$

(ii) Public key n $\quad$ private key (p, q)

(iii) Encryption $c = m^2 \bmod n$ for some msg $m \in \{1, \dots, n-1\}$

(iv) Decryption

Determine $x : x^2 \equiv c \pmod p$

$y : y^2 \equiv c \pmod q$

Determine $\left.\begin{aligned} f &\equiv x \pmod p \\ f &\equiv y \pmod q \end{aligned}\right\}$ by CRT see Chapter 9.1

But there are 4 solutions ▽

Note: $m >> \sqrt{n}$, otherwise compute square roots over the reals

Remark 9.5| Need to identify the correct solution out of 4

Remark 9.6| : a) Breaking is the same as factoring

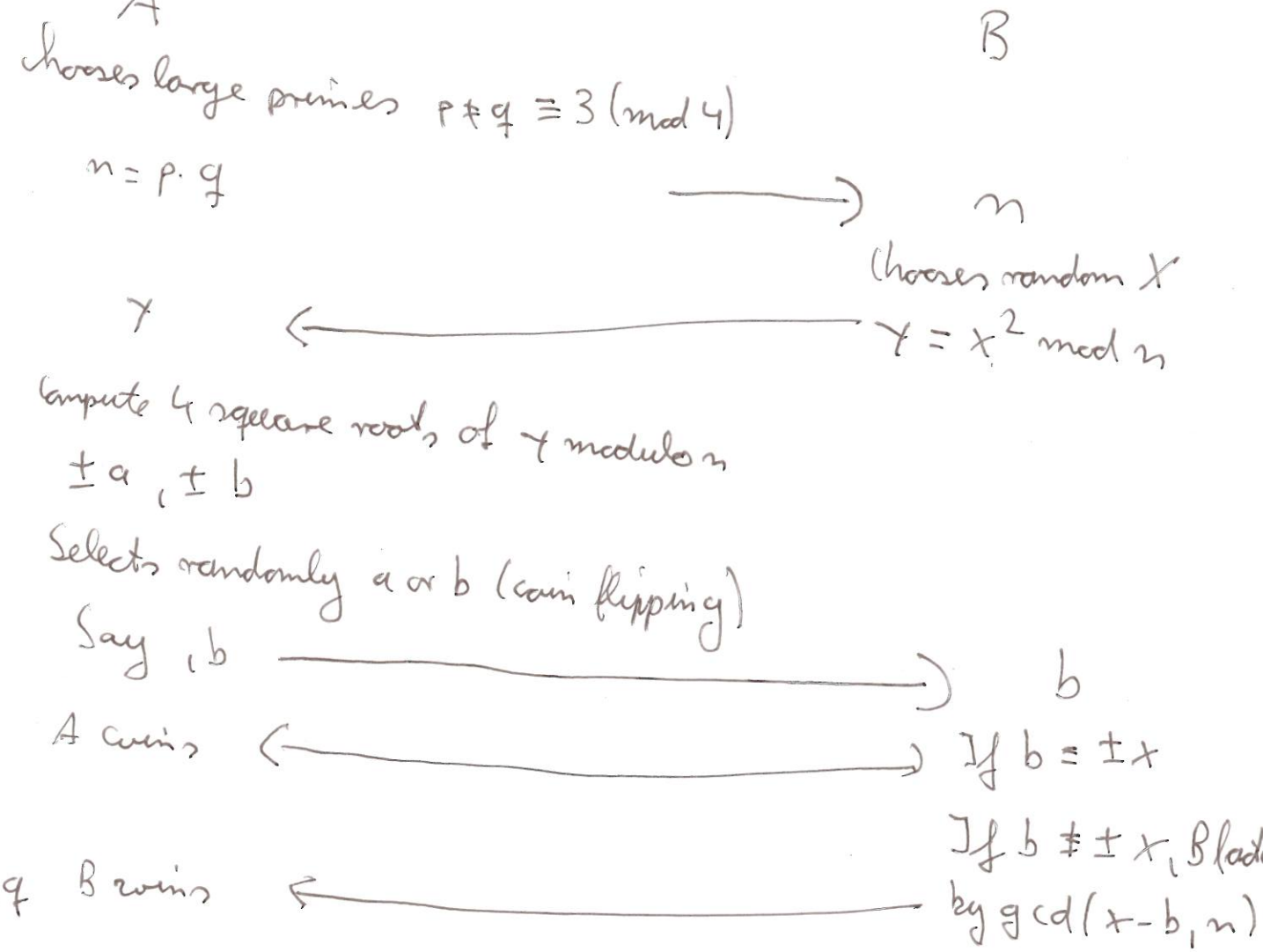
b) Vulnerable against chosen ciphertext attacks (analogously to the RSA side-channel attack)

c) Broadcasting: CRT may be applied (also for RSA with small e)

9.3 Flipping coins over the telephone

Alice and Bob want to decide over the telephone who gets a device offered by a friend. Alice flips a coin, Bob chooses "tails". Alice says "Sorry, it was Heads". She wins.
There are multiple opportunities for cheating.
Hence, a secure and fair protocol is sought.

Protocol



Security of Flipping Coin Protocol

a) A chooses n as a product of more than two primes, k primes,
- There are 2^k square roots, for $2^k - 2$ numbers B is able to factorize n $\Rightarrow$ A leaves her chances to win, but B could check that by checking the factors for primality, e.g by MRPT

b) A chooses a prime as n $\Rightarrow$ B could/should test n for primality

c) A does not choose primes $p, q \not\equiv 3 \pmod 4$
$\Rightarrow$ She can't calculate square roots or it is more difficult ($\rightarrow$ e),

d) B sends a random y
   i) y is no square : A does not find a root $\Rightarrow$ stop: B cheats
   ii) y is a QR : A finds a root, but B cannot factorize, A wins

e) A sends a random number z, not a root of y, B cannot factorize
B checks $z^2 \equiv y \pmod n$, if not $\rightarrow$ stop, A cheats

f) If B wants to lose, he can do so.

Example

A : $p = 19$, $q = 23$, $n = 437$ → B

B : random $x = 112$

$y = 112^2 \bmod 437 = 308$ → A

A : $a = 112$ $\quad -a = 325$

$b = 135$ $\quad -b = 302$

A : Selects b or -b

B : $\gcd(b - x = 135 - 112, 437) = 23$

or : $\gcd(-b - x = 302 - 112, 437) = 19$

→ B wins

A : selects a or -a

B cannot factor n