

Admin:

Pset #3 due 4/5

Take-home Quiz out 4/5 due 4/21

Projects!

Today:

Recap

DH model of PK cryptography

RSA: invention
method
correctness
security
factoring & RSA problem
OAEP
small d's
side channel
bad randomness
quantum

Readings:

DH paper

RSA paper

Boneh: 20 yrs of attacks on RSA

Recap:

\mathbb{Z}_p^* = group on $\{1, 2, \dots, p-1\}$ with mult. mod p

\mathbb{Z}_n^* = group on $\{a : 1 \leq a < n \text{ \& } \gcd(a, n) = 1\}$
using mult. mod n

modular exponentiation with repeated squaring

$m^e \pmod{n}$ e.g. for RSA

modular mpy's proportional to bit length of e

La Grange's Thm: $(\forall a \in G) a^{|G|} = 1$

PK crypt defs: $\text{Gen}(1^k) \rightarrow (\text{PK}, \text{SK})$

$\text{Enc}(\text{PK}, m) \rightarrow c$

$\text{Dec}(\text{SK}, c) \rightarrow m$

CPA & CCA security

Diffie-Hellman model of PK crypto

"New Directions in Cryptography" (Nov. 1976)

- $\text{Gen}(1^\lambda) \rightarrow (\text{PK}, \text{SK}, \mathcal{M}, \mathcal{C})$

(public key, secret key,
message space, ciphertext space)

Here $|\mathcal{M}| = |\mathcal{C}|$

- $\text{Enc}(\text{PK}, \cdot)$ is an efficient (poly-time) computable map that is one-to-one & deterministic from \mathcal{M} to \mathcal{C}

$c = \text{Enc}(\text{PK}, m)$ is (unique) ciphertext for m

- $\text{Dec}(\text{SK}, \cdot)$ is efficiently computable inverse

$$\text{Dec}(\text{SK}, c) = \text{Dec}(\text{SK}, \text{Enc}(\text{PK}, m)) = m$$

($\forall m \in \mathcal{M}$)

- It is hard/infeasible to decrypt with knowledge of PK but without knowledge of SK. SK represents "trapdoor" information that enables inversion of the (otherwise one-way) function $\text{Enc}(\text{PK}, \cdot)$.

D&H proposed model, but didn't have implementation!

RSA - invention (Rivest, Shamir, Adleman, 1977)

RSA method:

• Gen (1^λ):

find two large primes p, q of length λ
(e.g. $\lambda = 1024$ bits)

p, q could be randomly chosen to guard
against factoring attacks

$$n = p \cdot q$$

$$\varphi(n) = |\mathbb{Z}_n^*| = (p-1)(q-1)$$

$$e \leftarrow \mathbb{Z}_{\varphi(n)}^* \quad \text{e.g. } \gcd(e, \varphi(n)) = 1$$

$e = 65,537$ common choice

$$d = e^{-1} \pmod{\varphi(n)} \quad [\text{via Euclid's extended alg}]$$

$$PK = (n, e)$$

$$SK = (d, p, q)$$

$$M = \mathcal{C} = \mathbb{Z}_n \quad (\text{note: } \mathbb{Z}_n^* \neq \mathbb{Z}_n !)$$

• Enc (PK, m) = $m^e \pmod{n}$ ($\forall m \in \mathbb{Z}_n$)

• Dec (SK, c) = $c^d \pmod{n}$ ($\forall c \in \mathbb{Z}_n$)

Correctness of RSA

Lemma: (Chinese remainder theorem or CRT)

Let $n = p \cdot q$ where p, q are distinct primes.

$$(\forall x, y \in \mathbb{Z}_n)$$

$$x = y \pmod{n} \iff x = y \pmod{p} \ \& \ x = y \pmod{q}$$

Thus it suffices to prove RSA correct mod p . Correctness mod q is proved the same way & CRT \Rightarrow correctness mod n .

$$\left[\begin{array}{l} \text{Given } e \cdot d = 1 \pmod{\varphi(n)} \quad \text{since } d = e^{-1} \pmod{\varphi(n)} \\ \Rightarrow e \cdot d = 1 + t \cdot (p-1) \cdot (q-1) \quad \text{for some } t, \text{ over } \mathbb{Z} \\ \Rightarrow e \cdot d = 1 \pmod{(p-1)} \quad \text{i.e. } d = e^{-1} \pmod{p-1} \end{array} \right.$$

Correctness of RSA means

$$(\forall m \in \mathbb{Z}_n) \quad (m^e)^d = m \pmod{n}$$

By CRT we only need to prove

$$(\forall m \in \mathbb{Z}_p) \quad (m^e)^d = m \pmod{p}$$

We consider 2 cases:

Case 1: $m = 0 \pmod{p}$
 Trivial: $0^{ed} = 0 \pmod{p}$

Case 2: $m \neq 0 \pmod{p}$

$$\equiv m \in \mathbb{Z}_p^*$$

$$\text{so } m^{p-1} = 1 \pmod{p} \quad [\text{Fermat}]$$

$$\text{Then } m^{ed} = m^{1+u \cdot (p-1)} \pmod{p}$$

$$\text{where } u = t \cdot (q-1)$$

$$m^{ed} = m \cdot (m^{p-1})^u \pmod{p}$$

$$= m \cdot 1^u$$

$$\therefore \begin{cases} m^{ed} = m \pmod{p} & (\forall m \in \mathbb{Z}_p) \\ m^{ed} = m \pmod{q} & (\forall m \in \mathbb{Z}_q) \quad (\text{similarly}) \end{cases}$$

$$\Rightarrow m^{ed} = m \pmod{n} \quad (\forall m \in \mathbb{Z}_n) \quad (\text{CRT})$$

Thus $(\forall m \in \mathbb{Z}_n)$

$$\text{Dec}(\text{SK}, \text{Enc}(\text{PK}, m)) = m \quad \blacksquare$$

RSA is $\mathbb{1}$ to $\mathbb{1}$; $\text{Dec}(\text{SK}, \cdot)$ is the
 inverse of $\text{Enc}(\text{PK}, \cdot)$

Security of RSA

Factoring attack:

If an Adversary can factor n , then the Adversary can compute $\varphi(n)$, and thus compute $d = e^{-1} \pmod{\varphi(n)}$

Key insight: size $\varphi(n)$ of group \mathbb{Z}_n^* is unknown & unknowable to (bounded) Adversary.

How hard is factoring?

- time $\exp\{c \cdot (\ln n)^{1/3} (\ln \ln n)^{2/3}\}$
- RSA challenge RSA-250 factored 2020 (829 bits)
- RSA keys of ≥ 2048 bits secure for a long time, unless there are algorithmic breakthroughs (including possibility of building a quantum computer).

RSA problem

(Factoring being hard may not be enough)

RSA Problem (or RSA assumption)

Given $C = m^e \pmod{n}$, it is hard to find m .

Is RSA CPA secure?

No. (It is deterministic!)

∴ not CCA secure, either!

How to make RSA CCA secure?

"Pad" message with 0's & randomness,

using OAEP (Optimal Asymmetric Encryption Padding), then encrypt.

Decryption rejects if 0's not present.

OAEP:

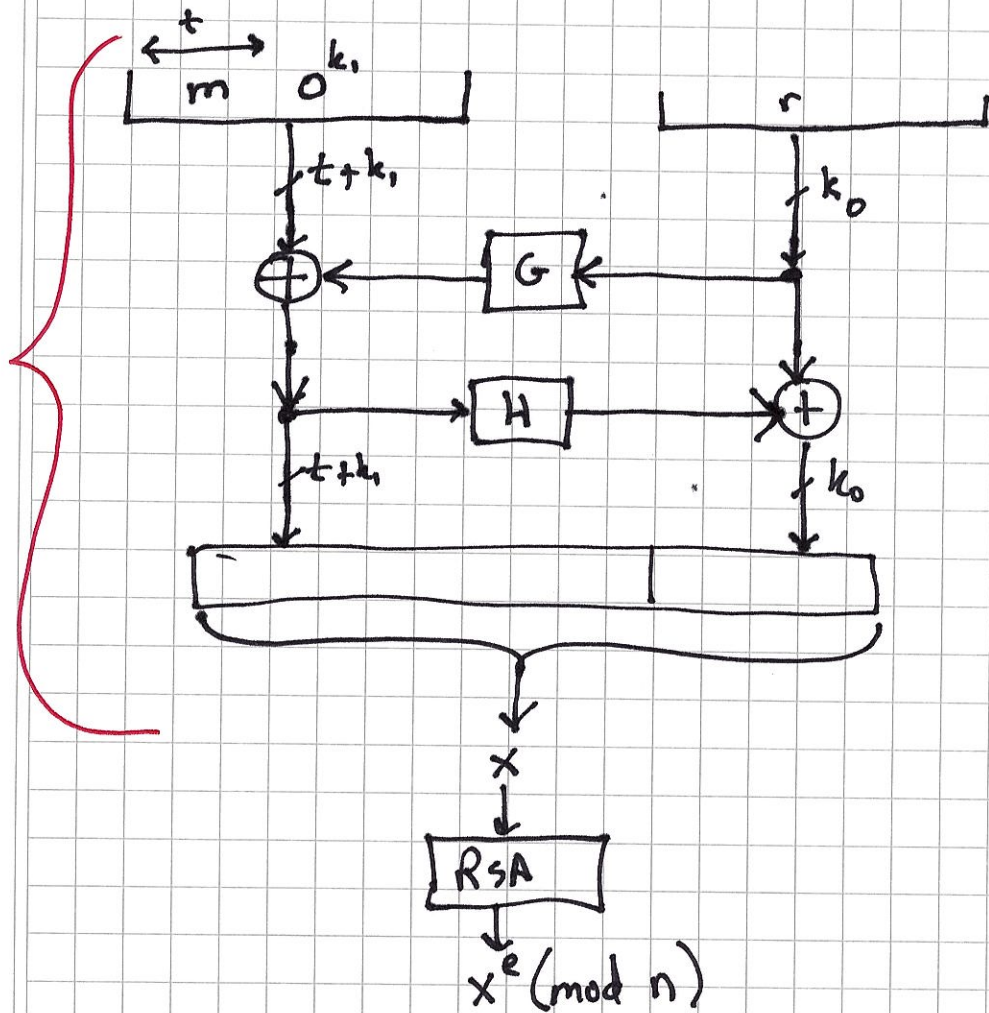
Let $t = |m|$

Let r be randomness of length k_0

Add k_1 bits of 0 s 0^{k_1} (to check)

Assume: $G: \{0,1\}^{k_0} \rightarrow \{0,1\}^{t+k_1}$
 $H: \{0,1\}^{t+k_1} \rightarrow \{0,1\}^{k_0}$ } are RO's

OAEP



On decryption: invert RSA
 invert OAEP
 reject if 0^{k_1} not present
 else output m

Theorem: RSA with OAEP is CCA secure, assuming ROM for G & H , & assuming RSA problem (RSA hard to invert on random inputs)

[Needs slightly modified assumptions, or OAEP⁺
for general trapdoor permutation, but OK with RSA]

OAEP used in practice.

Other aspects of RSA security

Weak keys

small d (e.g. $< n^{1/4}$) is insecure

Implementation:

Side channels: power
timing

Fault injection: (esp. if CRT is used)

Quantum computing

Peter Shor (MIT) has a polynomial-time factoring algorithm on a quantum computer.