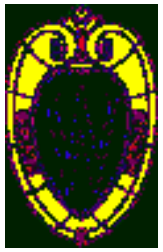


CS/ECE/Math 435
Introduction to Cryptography

Professor Chris DeMarco
Department of Electrical & Computer Engineering
University of Wisconsin-Madison

Spring Semester 2021

Recap Definition of RSA System from last lecture:

- A user selects two distinct, large prime numbers, p and q. Defin $N = p \cdot q$, and $\varphi = (p-1)(q-1)$.
- User next selects $d, e \leq N$ such that $\text{mod}(d \cdot e, \varphi) = 1$.

- Binary messages in this system are partitioned into blocks of k bits, with $2^k < N$. Hence each k-bit block has a representation as an integer $x \in \mathbb{Z}_N$; the block-by-block encryption operates on integers in $\mathbb{Z}_N$.

- Any block x sent to this user will be encrypted using the function:

$$y = E_{(N, e)}(x) = \text{mod}(x^e, N)$$

- The user decrypts using their internally secret key d:

$$D_{(N, d)}(y) = \text{mod}(y^d, N)$$

Public key / Private key Protocol for RSA - How the two classes of keys are used.

- Every potential recipient of messages must publish (i.e. make publically available to all potential senders) the recipient's public key pair, (N, e)

- But every recipient keeps d internally secret; d is never sent over any communication channel.

Consider a sender "B" wishing to securely communicate a message $\underline{X}$ to receiver "A." Sender B "looks up" A's public key pair (N, e), and performs encryption $E_{(N,e)}(\underline{X}) = \underline{Y}$.

Note that $\underline{Y}$'s encryption function is "tailored" especially for its intended recipient A.

For any unauthorized entity (the attacker) seeking to decrypt $\underline{Y}$, the public key pair is known. But unlike symmetric encryption algorithms, knowledge of (N, e) does not (directly, at least) define the decryption function.

Obvious Question for RSA: Is it true that decryption recovers the original plaintext? In other words,

$$\text{does } x \overset{?}{=} D_{(N,d)}\left(E_{(N,e)}(x)\right) \quad \forall x \in \mathbb{Z}_N$$

Not So Obvious Answer (based on what is known as "Fermat's Little Theorem"):

YES.

Fermat's "Little" Theorem

(aside: this theorem is "little" in contrast to what is known as Fermat's "Great" Theorem, often also termed Fermat's Last Theorem, which was not proven until 1995, 330 years after Fermat's death).

Theorem Statement:

If p is a prime number, then

$\mod(a^p, p) = \mod(a, p)$ for any integer a.

Proof is sketched in Bach notes p. 19-1

To show $x = D(E(x)) \mod N$, recall relations between integer parameters defining RSA:

i) $N = p \cdot q$

$\Rightarrow$ For any integer w, and $z \in \mathbb{Z}_N$, such that $\mod(w, N) = z$,

$\mod(w, p) = \mod(z, p)$

and

$\mod(w, q) = \mod(z, q)$

So in particular, let $w = x^{d \cdot e}$, and we have the fact that if $z = \mod(x^{d \cdot e}, N)$, then

$$\mod(x^{d \cdot e}, p) = \mod(z, p)$$

and

$$\mod(x^{d \cdot e}, q) = \mod(z, q)$$

(ii) $\mod\left(d \cdot e, \overbrace{[(p-1)\cdot(q-1)]}^{\varphi}\right) = 1$

$\Rightarrow \quad d \cdot e = 1 + \underbrace{\tilde{k}(q-1)}(p-1)$

$= 1 + k \cdot (p-1)$

So, let's suppose we apply encryption / decryption to $x \in \mathbb{Z}_N$, and obtain $z \in \mathbb{Z}_N$ (we hope $z = x$, but keep z a placeholder for now).

$$z = \mod\left(x^{de}, N\right)$$

Recall that

$$\text{mod}\left(d \cdot e, \underbrace{\varphi}_{(q-1)(p-1)}\right) = 1$$

$$\Rightarrow d \cdot e = 1 + \tilde{k} \cdot (q-1)(p-1)$$

for some integer $\tilde{k}$

$$= 1 + k \cdot (p-1) \quad ; \text{ with } k = \tilde{k}(q-1)$$

So re-write

$$x^{de} = x^{[1 + k \cdot (p-1)]}$$

(13) From the result proven in HW 10, Prob 3, given that $z = \text{mod}\left(x^{[1 + k\cdot(p-1)]}, N\right)$, it follows that:

$$\text{mod}(z,p) = \text{mod}\left(x^{[1 + k\cdot(p-1)]}, p\right)$$

$$= \text{mod}\Big(\text{mod}(x,p) \cdot \text{mod}\left(\text{mod}\left((x^{p-1})^k, p\right), p\right)$$

$$\text{mod}\left(\text{mod}\left(x^{p-1}, p\right), p\right)^k$$

Our goal is to show that all of these terms evaluate to 1 if $x \neq 0$.

$$\text{mod}\left(x^{-1}, p\right) \cdot \text{mod}\left(x^{p}, p\right)$$

by Fermat's Little Theorem

$$\text{mod}(x, p)$$

- If $x \neq 0$, then $\text{mod}(x, p)$ must be $\in Z_p^*$ (recall p is a prime number, so Z_p^* includes all integers > 0, $< p$). Then

$$\text{mod}\left(\text{mod}(x^{-1}, p) \cdot \text{mod}(x, p), p\right) = 1,$$

and we're left with

$$z = \text{mod}(x, p) \cdot 1$$

- And if $x = 0$, it is trivially true that

$$\underbrace{z}_{0} = \underbrace{\text{mod}(x, p)}_{0}$$

- We can repeat all of the steps above, interchanging q for p, to similarly conclude

$$z = \text{mod}(x, q)$$

So candidate decrypted block, z, satisfies

$$x = z + k_q \cdot q \quad \text{for some integer } k_q$$

and

$$x = z + k_p \cdot p \quad \text{for some integer } k_p$$

$$\Rightarrow \quad k_q \cdot q = k_p \cdot p$$

$$\Rightarrow \quad k_q \text{ is integer multiple of } p,$$

$$\text{i.e.} \quad k_q = k_N \cdot p$$

$$\Rightarrow \quad X = Z + k_N \cdot p \cdot q$$

$$= Z + k_N \cdot N$$

$$\Rightarrow \quad Z = \text{mod}(X, N)$$

Decrypted block Z matches plaintext block X, modulo N. DONE

Example

Choose: $\boxed{p = 3, \quad q = 17}$; $N = 3 \cdot 17 = 51$

$$\varphi = (p-1)(q-1) = 2 \cdot 16 = 32.$$

Choose: $d = 11$, $e = 3$

satisfies $\mod(d \cdot e, \varphi) = 1$ ✓

$$\mod(33, 32) = 1$$

Recall original message will be binary, partitioned into blocks of size k with $2^k < N$; so here $k = 5$, $2^k = 32$.

Hence a plaintext block will be interpreted as an integer $0 \leq x \leq 31$, and such an x guaranteed $\in \mathbb{Z}_N$.

Suppose $x = 2$.

Then

$$E_{(N,e)}(x) = \mod(2^3, 51) = 8 = y$$

$N = 51$, $e = 3$

$$D_{(N,d)}(y) = \mathrm{mod}(8^{11}, 51)$$

$$\begin{matrix} \| & \| \\ 51 & 11 \end{matrix}$$

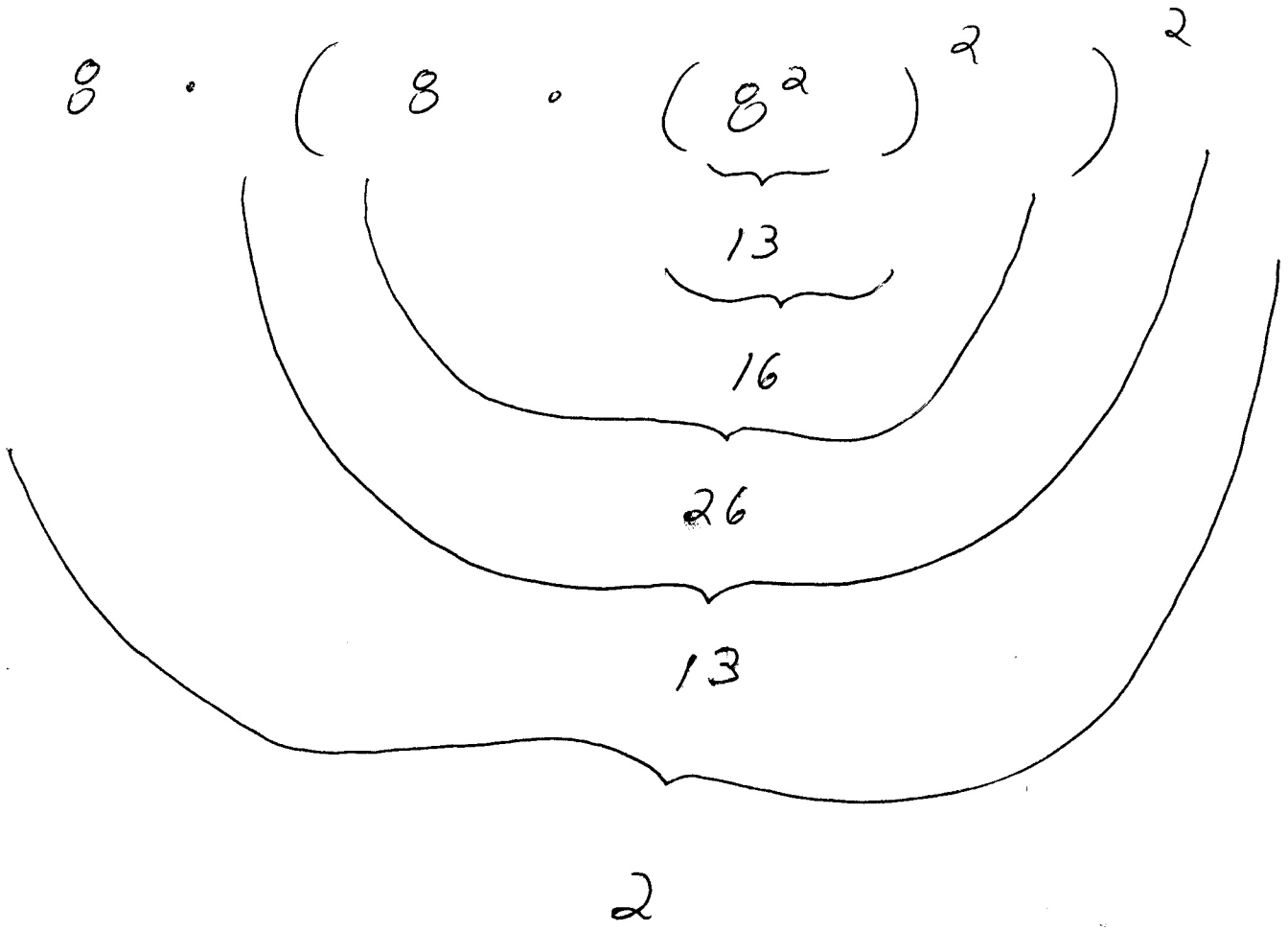
To compute, we may decompose

$$8^{11} = 8 \cdot 8^{10}$$

$$= 8 \cdot (8^5)^2$$

$$= 8\left(8 \cdot (8^2)^2\right)^2$$

evaluate each term mod 51


8 · (8 · (8²)²)²
13
16
26
13
2