LECTURE 7: CHAPTER 4: THE RSA CRYPTOSYSTEM FROM STILLWELL'S ELEMENTS OF NUMBER THEORY

NEEDED MATHEMATICAL INGREDIENTS

- ✓ inverses modulo n, Euler theorem $a^{\varphi(n)} \equiv 1 \mod (n)$
- ✓ algorithm to calculate binary rep. of #
- ✓ Euclidean algorithm which gives inverse of a mod b

RSA, preliminary sketch

$$\boxed{\text{message } m \in \mathbb{Z}} \xrightarrow[\text{modulo } (n)]{\text{exponentiated}} \boxed{m^e \,(\text{mod } n)} \xrightarrow[\text{mod } \cancel{\varphi(n)}\, n]{\text{exponentiated}} \boxed{(m^e)^d \mod \varphi(n)}$$

encryption: e and n publicly known

decryption: only easy if know e ~~$\varphi(n)$~~

§4.1: TRAPDOOR FUNCTIONS: (a bit on CRYPTOGRAPHY IN GENERAL)

Example: THE CAESAR CIPHER:

Take message $A\,B\,C\,D\,E \cdots Z \longrightarrow 1\,2\,3\,4\,5 \cdots 26$

then shift by adding k mod 26 so

$$ABCDE \cdots Z \longmapsto A+k, B+k, .., 26+k \mod 26$$

For example, $k = 3$,

$$ABCDE \cdots Z \longmapsto 45678 \cdots 3 \longleftrightarrow DEF \cdots C$$

So in this code ($k=3$ case)

$$A \longmapsto D$$
$$B \longmapsto E$$
$$\vdots$$
$$Z \longmapsto C$$

Remark: we ignore important issues such as how to parse words. Clearly this matters for real messages!

As Stillwell says "Go to Zagreb tomorrow"

$\longmapsto$ "Jr wr Cdjuhe wrpruurz"

Example 2: THE ONE-TIME PAD

Key: long sequence of #'s (x_i) in $\mathbb{N}_{26} = \{1, 2, \ldots, 26\}$
The digit x_i is added to i^{th} letter in message
then reciever must subtract x_i from i^{th} letter.
Once key is used then it's "torn off the pad"
and $x_{n+1}\ x_{n+2}, \ldots$ is used for next message.

Comment: both encryptor and decryptor need this huge key to make this work. However, once both possess it, this is nearly perfect security. In contrast, the Caesar cipher is way easier to put into practice, but far less secure.

COMPROMISE CIRCA 1970: the trapdoor functions. Basically, a trapdoor function is easy to do, but hard to undo.
As Stillwell mentions:
- like falling through trapdoor
- like scrambling eggs.

no key here.

Well, there's more, a trapdoor function is easy to undo with the help of a "key"

1976 • idea of trapdoor fncts.: Diffie and Hellman
1978 • RSA method: Rivest, Shamir, Adleman
1970's • Clifford Cocks (British Intelligence)

existence of key debated

What is the trap door?

Take primes which are big say P_1 and P_2 and multiply them $(P_1 P_2) \longmapsto n = P_1 P_2$. Now, given n find (P_1, P_2). Much harder,

$$\underbrace{n = f(P_1, P_2) = P_1 P_2}_{\substack{\text{polynomial time} \\ \sim n^2 \text{ steps for} \\ \text{pair of } n\text{-digit \#}}} \quad \text{vs} \quad \underbrace{f^{-1}(n) = (P_1, P_2)}_{\substack{\sim 10^n \text{ steps. To} \\ \text{factor a } n\text{-digit \#} \\ \text{basically have to divide} \\ n \text{ by the } 10^n \text{ \#s with} \\ \leq n \text{ digits}}}$$

$\underline{n=6}$ 36 vs. $10^6 = 1{,}000{,}000$

$\underline{n=9}$ 81 vs. $10^9 = 1{,}000{,}000{,}000$

etc...

<u>CAUSE FOR CAUTION</u>: 1994, SHOR showed a QUANTUM COMPUTER COULD FACTOR IN POLYNOMIAL TIME! This result casts a shadow on all the NP (non-polynomial) problems... perhaps a quantum computer will solve them in reasonable time, but, no feasible quantum computer constructed (YET...)

§ 4.2 INGREDIENTS OF RSA

To use RSA, one "owns" a pair of large primes, say P_1, P_2 of 100-digits $\Rightarrow P_1P_2$ takes about 100^2-steps to calculate, but $n = P_1P_2$ would take 10^{100}-steps to factor! It follows you can safely share $n = P_1P_2$ w/o revealing P_1, P_2.

Th^m/ Let P_1, P_2 be prime then $\varphi(P_1P_2) = (P_1-1)(P_2-1)$

Proof: $\varphi(P_1P_2)$ = # of natural #'s relatively prime to P_1P_2 and smaller than P_1P_2. Of course $\varphi(P_1) = P_1 - 1$ and $\varphi(P_2) = P_2 - 1$.

We need to count $a \in \mathbb{N}$ s.t. $\gcd(a, P_1P_2) = 1$.

Or, count the $a \in \mathbb{N}$ for which $\gcd(a, P_1P_2) \neq 1$

for example, $P_1, 2P_1, 3P_1, \dots, (P_2-1)P_1 < P_1P_2$ *

and $P_2, 2P_2, 3P_2, \dots, (P_1-1)P_2 < P_1P_2$. ** Stillwell claims these are the only exceptions to $\gcd(a, P_1P_2) = 1$.

If $\gcd(a, P_1P_2) = c$ $\Rightarrow$ ~~$c \mid a$ and $c \mid P_1P_2$~~
$\Rightarrow c \mid a$ and $c \mid P_1P_2$
$\Rightarrow c \mid a$ and $c \mid P_1$ or $c \mid P_2$

Hence Stillwell's claim correct by Prime divisor property.

Thus, the # of relatively prime # $< P_1P_2$ to P_1P_2 are

$$\begin{aligned}\varphi(P_1P_2) &= P_1P_2 - (P_2-1) - (P_1 - 1) - 1 \\ &= P_1P_2 - P_1 - P_2 + 1 \\ &= (P_1-1)(P_2-1). \quad //\end{aligned}$$

← don't include P_1P_2 itself start with $P_1P_2 - 1$ then remove * and **

$\boxed{Th^{m}/\ \varphi(P_1P_2) = \varphi(P_1)\varphi(P_2) = (P_1-1)(P_2-1)}$ ← multiplicative property of Euler φ-function.

application: If we know P_1 and P_2 (primes) then we can easily compute $n = P_1P_2$ and $\varphi(n) = (P_1-1)(P_2-1)$.

Also, choose encryption exponent e with $\gcd(e, \varphi(n)) = 1$ this $\#e$ and $\#n$ are made public so anyone can send encrypted messages to the user who knows P_1, P_2 (separately). Notice, once you encrypt M you can't undo it (unless you also know P_1, P_2, which you can't know with just $n = P_1P_2$)

From $\varphi(n)$ the user (with P_1, P_2) is able to compute a decryption exponent d which is inverse to e mod $\varphi(n)$.
Recall, by Euclidean Alg, $\gcd(e, \varphi(n)) = 1 \Rightarrow \exists m_1, m_2$ s.t. $m_1 e + m_2 \varphi(n) = 1 \Rightarrow [e]^{-1} = [m_1]$ w.r.t modulus $\varphi(n)$.

§4.3 Exponentiation mod n

$$m^h = \underbrace{m \cdot m \cdot \ldots m}_{h\text{-factors}} \longrightarrow (h-1)\text{-multiplications of } 100 \text{ digit \#'s} = ☹$$

But, can use binary form of h to guide slick exponentiation by successive squarings

Ex) m^{65} ~~$\Rightarrow m^{64} m = (m^8)^8 m = m$~~ $(65)_2 = (2^6 + 1)_2 = 1000001$

$$m \xrightarrow{S} m^2 \xrightarrow{S} m^4 \xrightarrow{S} m^8 \xrightarrow{S} m^{16} \xrightarrow{S} m^{32} \xrightarrow{S} m^{64} \xrightarrow{M} m^{65}$$

number of operations $\sim 2\,\#$ of binary digits in $h \sim \log_2(h) + 1$.
Still too huge w/o reduction... this is where mod(n) comes into play

Ok, so, to recap, we take message m and exponentiate via k by successive squarings with a few multiplications. For 100-digit primes $\Rightarrow m^k$ takes about 200 operations. If we do these modulo n then we have about n^2-steps per op. $\hookrightarrow 200 \cdot n^2$ total steps.

§4.4 RSA encryption and decryption

1 ▸ user's primes P_1, P_2 whose product $n = P_1 P_2$ is huge.

2 ▸ $m \in \mathbb{N}$ codes some message by simple transcription and $m < n$ as to not lose info mod n. (otherwise have to chop the message into smaller parts to encrypt w.r.t. key n.

3 ▸ $m \longmapsto m^e \pmod n$ where $\underbrace{\gcd(e, n) = 1}$. he said $\varphi(n)$ on p. 70 maybe this is typo on 72.

4 ▸ $m^e \longmapsto (m^e)^d \bmod n$

$ed + c_1\varphi(n) = 1$

$\hookrightarrow ed \equiv 1 \bmod \varphi(n)$.

$$(m^e)^d = m^{1 + c_1\varphi(n)} = m\left(m^{\varphi(n)}\right)^{c_1} = m$$

by Euler's Thm

$$m^{\varphi(n)} \equiv m \pmod n.$$

§4.5 Digital Signatures

- pick common message m (say Psalm 23 etc.)
- encrypt by key n and expon. e
- await user to decrypt m and send back

– [if user can uncover m then this proves they are the genuine owner of the key n with exp. e.]–

THE BINARY EXPONENTIATION TRICK

m^{49}

$49 = 32 + 16 + 1$

$(49)_2 = 110001$

① ② ③ ④ ⑤ ⑥

$$1 \longmapsto m \underset{①}{\Longrightarrow} m^2 \longrightarrow m^3 \underset{②}{\Longrightarrow} m^6 \underset{③}{\Longrightarrow} m^{12} \underset{④}{\Longrightarrow} m^{24} \underset{⑤}{\Longrightarrow} m^{48} \underset{⑥}{\longrightarrow} m^{49}$$

start with 1, of course could start with m^2 and go from ② ...

last step no square after m multiplication

GOAL: 5^{49} mod 221 : follow ①, ②, .., ⑥ above.

$$5 \underset{①}{\longmapsto} 5^2 \longmapsto 125 \underset{②}{\longmapsto}$$

$(125)^2 = 5^6$

$(-96)^2 = 5^6$

$155 = 5^6$

$\Rightarrow 5^6 = -66$

$\underset{③}{\longrightarrow}$

$5^{12} = (-66)^2$

$= 4356$

$= 157 \mod 221$

$= -64$

- divide by 221
- subtract off whole # part
- multiply by 221 to find remainder.

$④ \longmapsto$

$5^{24} = (-64)^2 \mod 221$

$= 118$

$\underset{⑤}{\longrightarrow}$

$5^{48} = (118)^2 \mod 221$

$= 1$

so annoying!

$\underset{⑥}{\longrightarrow}$

$5^{49} = 5(1)$

$= 5$