This is based on Chapter 4 of Lewand & Chapter 6 of Trappe and Washington
ON TO RSA

(We’ll pick up on DES and AES later.)

Symmetric Cryptosystems

A and B have a shared secret — the value of the key

\[ A = \text{amazon.com} \quad B = \text{book buyer} \]

\[ A \overset{\text{key}}{\Rightarrow} c \overset{\text{key}}{\Rightarrow} p \quad B \]

Asymmetric Cryptosystems

A and B have no shared private info — but they want to communicate securely.

Public key Cryptosystems

Break the key into two parts: \( k_{\text{pub}} \) and \( k_{\text{priv}} \)

Each party has her/his key pair
PKC: THE SETUP

Alice
\[ E_A \text{ Alice’s public encryption key} \]
\[ D_A \text{ Alice’s private decryption key} \]

Bob
\[ E_B \text{ Bob’s public encryption key} \]
\[ D_B \text{ Bob’s private decryption key} \]

Encryption
\[ \text{encrypt}(K,p) = c \]

Decryption
\[ \text{decrypt}(K,c) = p \]
PKC: THE EXCHANGE PHASE

Alice wants to send \( m \) to Bob

Alice

1. Looks up \( E_B \).
2. Computes \( c = \text{encrypt}(E_B, m) \).
3. Sends \( c \) over an open channel.

Bob

1. Receives \( c \).
2. Computes \( m = \text{decrypt}(D_B, c) \).

Eve

1. Captures \( c \).
2. Now what?
   To build a PKC, we need some more number theory
EULER’S PHI FUNCTION

\( \varphi: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+ \).

\[ \varphi(n) = \| \{ m \in \mathbb{Z}^+ : m < n \& \gcd(m, n) = 1 \} \| \]

= the number of positive integers < \( n \) relatively prime to \( n \)

CONVENTION: \( \varphi(1) = 1 \).

\( \varphi(5) = \| \{ 1, 2, 3, 4 \} \| = 4. \)

\( \varphi(6) = \| \{ 1, 2, 3, 4, 5 \} \| = 2. \)

\( \varphi(12) = \| \{ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 \} \| = 4. \)
LEMMA 4.1
Suppose $p$ is a positive prime. Then $\varphi(p) = p - 1$.

Proof

LEMMA 4.2
Suppose $p$ and $q$ are distinct primes.
Then $\varphi(p \cdot q) = (p - 1) \cdot (q - 1) = \varphi(p) \cdot \varphi(q)$.

Proof
Let

$S = \{ m \in \mathbb{Z}^+ : m < p \cdot q \} = \{ 1, 2, 3, \ldots, pq - 1 \}$.

$M_p = \{ p, 2p, 3p, \ldots, (q - 1)p \} \subseteq S$.

$M_q = \{ q, 2q, 3q, \ldots, (p - 1)q \} \subseteq S$.

CLAIM 1: $M_p \cap M_q = \emptyset$.

CLAIM 2: $\varphi(p \cdot q) = \| S - M_p - M_q \| = (p - 1) \cdot (q - 1)$. 
LEMMA 4.3
Suppose \( p \) is a positive prime and \( k > 0 \).
Then \( \gcd(p^k, n) = 1 \iff p \nmid n \).

Proof proof on board

LEMMA 4.4
Suppose \( p \) is a positive prime and \( k > 0 \).
Then \( \varphi(p^k) = p^k - p^{k-1} \).

Proof proof on board

LEMMA 4.5
Suppose \( a, b, c \in \mathbb{Z} \).
Then \( \gcd(a, b \cdot c) = 1 \iff \gcd(a, b) = 1 \text{ and } \gcd(a, c) = 1 \).

Proof Use \( \gcd(u, v) = 1 \iff (\exists x, y)[ux + vy = 1] \).
LEMMA 4.6
Suppose $m, n \in \mathbb{Z}^+$ and $\gcd(m, n) = 1$.
Then $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Proof proof on board

LEMMA 4.7
Suppose $n > 1$ has prime factorization:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r},$$

where $k_1, \ldots, k_r \geq 1$. Then

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}).$$

Proof proof on board
LEMMA 4.8
Suppose $n > 2$. Then $\varphi(n)$ is even.

Proof
(proof on board)

LEMMA 4.9
Suppose

$\triangleright n > 1$.

$\triangleright \{a_1, a_2, \ldots, a_{\varphi(n)}\} = \{x : 1 \leq x < n \& \gcd(n, x) = 1\}$.

$\triangleright \gcd(n, a) = 1$.

Then

$(a \cdot a_1) \mod n, (a \cdot a_2) \mod n, \ldots, (a \cdot a_{\varphi(n)}) \mod n$

is a permutation of $a_1, a_2, \ldots, a_{\varphi(n)}$.

Proof
(proof on board)
EULER’S THEOREM

THEOREM
Suppose $a, n \in \mathbb{Z}^+$ with $\gcd(a, n) = 1$.
Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof

COROLLARY
Suppose $a, n \in \mathbb{Z}^+$ with $\gcd(a, n) = 1$.
Then $a^{\varphi(n)-1} \equiv a^{-1} \pmod{n}$.

COROLLARY (Fermat’s Little Lemma)
Suppose $p$ is prime and $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{n}$.

EULER’S COROLLARY
Suppose $p$ and $q$ are distinct primes and $\gcd(a, pq) = 1$.
Then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$. 
THE RSA ALGORITHM: SETUP

Alice:

1. Picks two large primes $p$ & $q$.
2. Computes $n = p \cdot q$ and $\varphi(n) = (p - 1) \cdot (q - 1)$.
3. Picks $e \in \{ 1, \ldots, \varphi(n) - 1 \}$ with $\gcd(e, \varphi(n)) = 1$.
4. Computes $d \in \{ 1, \ldots, \varphi(n) - 1 \}$ with $d \cdot e \equiv 1 \pmod{\varphi(n)}$. (How?)
5. Publishes $e$ and $n$.
   She keeps $d$, $p$, $q$, and $\varphi(n)$ secret.

Bob:

Does the same thing.
THE RSA ALGORITHM: THE PROTOCOL

Bob wants to send Alice a message.

Bob

1. Converts a message to a number $m$. \text{(Assume $0 \leq m < n$.)}
2. Computes $c = m^e \mod n$.
3. Sends $c$ to Alice.

Alice

1. Receive $c$.
2. Computes $m' = c^d \mod n$. \textbf{Claim:} $m = m'$.
3. Converts $m'$ to a text message.

Lots of questions to address. First the claim.
PROVING THE CLAIM

THEOREM 4.1

Suppose

\( p \) and \( q \) are distinct primes.
\( n = p \cdot q \)
\( e \in \{ 1, 2, \ldots, \varphi(n) - 1 \} \) with \( \gcd(e, \varphi(n)) = 1 \).
\( d \in \{ 1, 2, \ldots, \varphi(n) - 1 \} \) with \( d \cdot e \equiv 1 \pmod{\varphi(n)} \).
\( c = m^e \pmod{n} \).
\( m' = c^d \pmod{n} \).

Then, \( m' = m \).

Proof \( m' = c^d \pmod{n} = (m^e)^d \pmod{n} = m^{e \cdot d} \pmod{n} \).

CLAIM. \( m \equiv m^{e \cdot d} \pmod{p} \). proof on board
CLAIM. \( m \equiv m^{e \cdot d} \pmod{q} \). proof on board
CLAIM. \( m \equiv m^{e \cdot d} \pmod{n} \). proof on board
HOW DO WE COMPUTE $e^{-1} \mod \varphi(n)$?

- Recall that $\gcd(e, \varphi(n)) = 1$.
- Hence, there are $x$ and $y$ such that
  $$x \cdot e + y \cdot \varphi(n) = 1.$$  
- Therefore,
  $$1 = (x \cdot e + y \cdot \varphi(n)) \mod \varphi(n) = (x \cdot e) \mod \varphi(n).$$
- So, $x \equiv e^{-1} \mod \varphi(n)$.
- We want the multiplicative inverse for a given modulus.
EXTENDED EUCLID’S ALGORITHM

Perform Euclid’s Algorithm as before, but keep notes along the way.

Start with:

- \( a = qb + r \).
- \( \exists s, t \ni as + bt = \gcd(a, b) \).
- Note: \( a = 1 \cdot a + 0 \cdot b \)
  
  \( b = 0 \cdot a + 1 \cdot b \)

- Multiply the second by \( q \) and subtract from the first:
  
  \( r = 1 \cdot a + (-q) \cdot b \)

- Then, perform another step of Euclid’s algorithm on the new \( b \) and \( r \), aggregating the results.
EXTENDED EUCLID’S ALGORITHM, II

\[
s_0 = 1 \quad t_0 = 0
\]
\[
s_1 = 0 \quad t_1 = 1
\]
\[
a = s_0 \cdot a + t_0 \cdot b
\]
\[
b = s_1 \cdot a + t_1 \cdot b
\]
\[
q_{i+1} = \text{int} \left( \frac{r_{i-1}}{r_i} \right)
\]
\[
r_{i+1} = r_{i-1} \mod r_i
\]
\[
s_{i+1} = s_{i-1} - (q_{i+1} \cdot s_i)
\]
\[
t_{i+1} = t_{i-1} - (q_{i+1} \cdot t_i)
\]

Stop when \( r_i = 1 \), and \( t_i \) is the answer!
Example: find multiplicative inverse of $53 \text{ mod } 179$
(Note: $a = 179, b = 53$).

\[
\begin{array}{cccc}
   q_i & r_i & s_i & t_i \\
   0 & - & 179 & 1 & 0 \\
   1 & - & 53 & 0 & 1 \\
   2 & 3 & 20 & 1 & -3 \\
   3 & 2 & 13 & -2 & 7 \\
   4 & 1 & 7 & 3 & -10 \\
   5 & 1 & 6 & -5 & 17 \\
   6 & 1 & 1 & 8 & -27 \\
\end{array}
\]

$53^{-1} \text{ (mod } 179) \equiv -27 \equiv 152 \text{ (mod } 179)$
HOW DO WE COMPUTE $m^e \pmod{n}$?

Remember $m$, $e$, & $n$ are 200+ digits. So $m^e$ is huge.

**Trick 1** Compute mod $n$

*Claim:* Suppose $n \geq 1$, $a, b, c \in \mathbb{Z}$

(a) $(a + b) \pmod{n} = ((a \pmod{n}) + (b \pmod{n})) \pmod{n}$.

(b) $(a \cdot b) \pmod{n} = ((a \pmod{n}) \cdot (b \pmod{n})) \pmod{n}$.

**Trick 2** Use the repeated squaring trick ($\approx 1500$ years old)

$\blacktriangleright m^0 = 1$.

$\blacktriangleright m^{2e} = (m^e)^2$.

$\blacktriangleright m^{2e+1} = m \cdot (m^e)^2$. 
MORE WORRIES ABOUT RSA

Q: How do we find those big primes? (later)

Q: Is RSA secure?

A: No one knows.

Q: Why is it believed to be secure?

A: It is based on the belief that factoring is hard.

Eve

knows $n$ and $e$ since these are public

If she can factor $n = p \cdot q$,

then $d = (e^{-1} \mod (p - 1)(q - 1))$.

Maybe there is a shortcut from $n$ and $e$?

No!
WHY KEEP $\varphi(N)$ SECRET?

If we know $n$ and $\varphi(n)$:

- $n = p \cdot q$
- $\varphi(n) = (p - 1)(q - 1) = pq - p - q + 1$
- $s = n - \varphi(n) + 1 = p + q$
- $s^2 = p^2 + 2pq + q^2$
- $s^2 - 4n = p^2 - 2pq + q^2 = (p - q)^2$

Therefore, we know $p + q$ and $p - q$, so we can solve for $p$ and $q$.

See T&W, p. 141.
CLAIM
Finding the decryption exponent \( (d) \) is about as hard as factoring.

Why? Suppose there is an alg. \( A \) such that \( A(n, e) = d \).
Then there is a probabilistic algorithm for factoring \( n \) that is not much more expensive than \( A \) and such that

\[
\begin{align*}
\text{it gives the correct answer with prob.} & \geq \frac{1}{2}. \\
\text{it gives no answer with prob.} & \leq \frac{1}{2}
\end{align*}
\]

COROLLARY
If \( d \) becomes public, you should choose a new \( n \). (Why?)
YET MORE RSA ATTACKS

Choosing $d$ and $e$ too small is trouble. (T&W, p142 and 143)

**THEOREM** (Wiener) Suppose:

- $n = p \cdot q$, $p$ and $q$ primes, and $q < p < 2q$.
- $d < \frac{1}{3} \cdot n^{1/4}$.
- $d \cdot e = 1 \pmod{\varphi(n)}$.

Then, there is a polytime alg. for finding $d$ from $n$ and $e$.

**THEOREM** (Boneh) Suppose:

- $(n, e)$ is an RSA pub. key and $d \cdot e \equiv 1 \pmod{\varphi(n)}$.
- $n$ has $m$ binary digits.

Then, there are algs. that given the last $m/4$ digits of $d$ or the first $m/4$ digits of $d$, constructs all of $d$ in $O(e \log_2 e)$ time. (If $e$ is small, fast. If $e$ is large, too slow.)
FINDING PRIMES

FACT  There are lots of primes to find.

THE PRIME NUMBER THEOREM
Let \( \pi(n) = \) the number of primes in \( \{1, \ldots, n\} \). Then

\[
\lim_{n \to \infty} \frac{\pi(n)}{n / \log e n} = 1.
\]

(That is, \( \pi(n) \approx n / \log e n \).

Observation  Suppose \( k \in \{1, \ldots, n\} \) is (uniformly) randomly picked. Then

\[
Pr[k \text{ is prime}] = \frac{\# \text{ of primes}}{\# \text{ of possible } k} \approx \frac{n / \log e(n)}{n} = \frac{1}{\log e n}
\]

Example  For 512 bit numbers, \( \frac{1}{\log e(2^{512})} \approx \frac{1}{400} \) (not bad!)
THEOREM (Agrawal, Kayal, Saxana — August 2002)
There is a deterministic $O((\log e n)^{12+\epsilon})$ time algorithm for testing if $n$ is a prime.

THEOREM (Lenstra and Pomerance 2003)
$O((\log e^{12+\epsilon})) \rightarrow O((\log e^{6+\epsilon})).$

Observation. $O(n^{6+\epsilon})$ is not cheap.
Primality testing doesn’t help much with factoring.

By Fermat’s Little Lemma

If $n$ is prime, then for all $b$ with $\gcd(n, b) = 1$

$$b^{n-1} \equiv 1 \pmod{n}.$$  \hfill (⋆)

Example  For $n = 91$ and $b = 3, 2$.

$3^{90} \equiv 1 \pmod{91}$.  \hfill $2^{90} \equiv 64 \pmod{91}$.

FACT

If $n$ is not prime, then (⋆) is possible but not likely.

The fact is the basis of the practical, probabilistic primality tests.
PRIMALITY TESTING, PSEUDO-PRIMES

DEFINITION

(a) \( \mathbb{Z}_n^* = \{ a : 1 \leq a < n \& \gcd(a, n) = 1 \} \).

(b) Suppose \( b \in \mathbb{Z}_n^* \). The order of \( b \) in \( \mathbb{Z}_n^* \) is the smallest positive number \( k \) such that
\[
b^k \equiv 1 \pmod{n}.
\]

(c) Suppose \( n \) is an odd composite number and \( b \) is \( \exists \) \( \gcd(n, b) = 1 \) and
\[
b^{n-1} \equiv 1 \pmod{n}.
\]

We call such an \( n \) a pseudo-prime to the base \( b \).
Proposition  Let $n$ be an odd composite number.

(a) Suppose $\gcd(n, b) = 1$. Then:

$n$ is a pseudo-prime to the base $b$ iff

(the order of $b$ in $\mathbb{Z}_n^*$)$|(n - 1)$

(b) Suppose $b_1, b_2 \in \mathbb{Z}_n^*$ and $n$ is a pseudo-prime to the bases $b_1$ and $b_2$. Then $n$ is also a pseudo-prime to the bases $b_1 \cdot b_2 \mod n$ and $b_1 \cdot b_2^{-1} \mod n$.

(c) Suppose $n$ fails the test $[b^{n-1} \equiv 1 \pmod{n}]$ for at least one $b \in \mathbb{Z}_n^*$. Then $n$ fails the test for at least $\frac{1}{2}$ the $b \in \mathbb{Z}_n^*$. 
TESTING FOR PRIMES AND CARMICHAEL NUMBERS

Test \((n,k)\)

repeat \(k\) times

Choose \(b \overset{\text{ran}}{\in} \{1, \ldots, n-1\}\).

Set \(d := \gcd(b, n)\).

If \((d > 1)\) or \(b^{n-1} \not\equiv 1 \pmod{n}\)

then return \textbf{REJECT} \hspace{1cm} (* \(n\) is composite *)

end repeat

return \textbf{ACCEPT} \hspace{1cm} (* \(n\) is a prime or p.p. to many bases *)

end Test

▶ If \(n\) fails Test\((n,k)\), then \(n\) is composite.

▶ If \(n\) passes Test\((n,k)\), then

\[
\text{Prob}[n \text{ is prime or a Carmichael number}] \geq 1 - 2^{-k}.
\]
A Carmichael Number $n$:

- is odd
- is composite
- satisfies Fermat’s Little Theorem, i.e.:

$$\forall a \in \mathbb{Z^+} \exists \gcd(a, n) = 1,$$

$$a^{n-1} - 1 \equiv 0 \pmod{n}$$

In other words, if you go into Africa looking for elephants, but all you test for is multi-ton gray animals, you might find elephants, but then again, you might find rhinos.
THE MILLER-RABIN PRIMALITY TEST

DEFINITION Suppose $n$ is an odd composite number and that $s$ and $t$ are such that $(n - 1) = 2^s \cdot t$ where $t$ is odd

$n - 1 = 1 \ldots 1 \ 00 \ldots 0$

$t$ in binary $s$ many 0s

Example $n = 21$ / $n - 1 = 20 = 10100_2$ / $s = 2$ / $t = 5$

DEFINITION $n$ is a strong-pseudoprime to the base $b \in \mathbb{Z}_n^*$ iff $n$ and $b$ satisfy:

$b^t \equiv 1 \pmod{n}$

$b^{2^r t} \equiv -1 \pmod{n} \quad r \in \{0, 1, \ldots, s - 1\}$

PROPOSITION If $n$ is an odd composite number, then $n$ is a strong-pseudoprime to the base $b$ for at most 25% of the $b \in \mathbb{Z}_n^*$. Proof omitted
**MILLER-RABIN, CONTINUED**

Procedure Miller-Rabin(n,k)

Find $s$ and $t \ni n - 1 = 2^s t$ with $t$ odd.

repeat $k$ times

Choose $b \overset{\text{ran}}{\in} \mathbb{Z}_n^*$.

If not MR(n,s,t,b) then return REJECT (* $n$ is composite *)

end repeat

return ACCEPT (* $n$ is prime with prob. $\geq (1 - (\frac{1}{4})^k)$ *)

Procedure MR(n,s,t,b)

If $b^t \equiv \pm 1 \pmod{n}$ then return true

Set $c \leftarrow b^t \pmod{n}$.

For $r \leftarrow 1, \ldots, s - 1$ do

$c \leftarrow (c^2 \pmod{n})$

If $c = -1$ then return true

return false
FACTORYING: POLLARD’S (P-1) METHOD

Factors $n$ when there is a $p|n$ such that

$p - 1$ has only small prime factors.

Pollard’s (p-1) Method

Choose $a > 1$. (Say $a=2$.) Choose $B \in \mathbb{N}$.

Set $b \leftarrow a$; For $j \leftarrow 1, \ldots, B$ do $b \leftarrow b^j \mod n$

(* At the end $b = a^B! \mod n$ *)

Set $d \leftarrow \gcd(b - 1, n)$

If $1 < d < n$ then return $d$ else return failure.

Obs If P’s method returns $d$ with $1 < d < n$, then $d|n$.

Heuristic Suppose $p|n$ and $p - 1$ has just small prime factors.

Then $p|B!$ is likely.

Suppose $B! = (p - 1) \cdot k$

By F’s Little Lemma, $a^{B!} = (a^{p-1})^k \equiv 1 \pmod{p}$.

Therefore, $p|(a^{B!} - 1)$ and $p|((a^{B!} \mod n) - 1)$.

Therefore, $p = \gcd(a^{B!} \mod n, n)$. 

— 31 —
FACTORIZATION, CONTINUED

<table>
<thead>
<tr>
<th>METHOD</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quadratic sieve</td>
<td>$O(e^{(1+o(1))}\sqrt{(\log n)(\log \log n)})$</td>
</tr>
<tr>
<td>Elliptic curve</td>
<td>$O(e^{(1+o(1))}\sqrt{2(\log p)(\log \log p)})$ (*)</td>
</tr>
<tr>
<td>Number field sieve</td>
<td>$O(e^{(1.92+o(1))}(\log n)^{1/2}(\log \log n)^{2/3})$ (*)</td>
</tr>
</tbody>
</table>

(*) $p = \text{a small prime factor}$

THEOREM (Peter Shor mid 1990s)
There is a polytime factoring algorithm — that runs on a quantum computer

Result (IBM 2002)
$15 = 3 \cdot 5$. 
Example

Q: What are the $x$’s that satisfy?

\[ x \equiv 2 \pmod{5} \]
\[ x \equiv 3 \pmod{7} \]
\[ x \equiv 4 \pmod{11} \]

A: \[ x = 385 \cdot k + 367 \text{ where } k = \mathbb{Z} \quad (385 = 5 \cdot 7 \cdot 11). \]

The Chinese Remainder Thm (Trad.) (Andrews p66)

Suppose \( m_1, m_2, \ldots, m_k \in \mathbb{Z}^+ \) are pairwise rel. prime (?)

Suppose \( b_1, \ldots, b_k \in \mathbb{Z} \)

Suppose \( M = m_1 \cdot \ldots \cdot m_k \).

Then the congruences

\[ x \equiv b_1 \pmod{m_1} \quad \ldots \quad x \equiv b_k \pmod{m_k} \]

have a unique solution mod \( M \).
THE CHINESE REMAINDER THEOREM, MODERN FORM

DEFINITION

\[ \mathbb{Z}_m = \text{def} \{ 0, \ldots, m - 1 \} . \]
\[ a +_m b = \text{def} (a + b) \mod m, \text{ where } a, b \in \mathbb{Z}_m \]
\[ a \times_m b = \text{def} (a \cdot b) \mod m, \text{ where } a, b \in \mathbb{Z}_m \]
\[ \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k} = \text{def} \{ (a_1, \ldots, a_k) : a_1 \in \mathbb{Z}_{m_1}, \ldots, a_k \in \mathbb{Z}_{m_k} \} \]
\[ (a_1, \ldots, a_k) + (b_1, \ldots, b_k) = \text{def} (a_1 + m b_1, \ldots, a_k + m b_k) \]
\[ (a_1, \ldots, a_k) \times (b_1, \ldots, b_k) = \text{def} (a_1 \times_m b_1, \ldots, a_k \times_m b_k) \]

THEOREM

Suppose \( M = m_1 \cdot \ldots \cdot m_k \) where the \( m_i \)'s are pairwise rel. prime.
Suppose \( f : \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k} \) is given by
\[
 f(a) = (a \mod m_1, a \mod m_2, \ldots, a \mod m_k) .
\]

THEN \( f \) is a ring isomorphism between \( \mathbb{Z}_M \) and \( \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k} \).

proof on board

Q: What in the world is a ring isomorphism?
Q: What does this have to do with the traditional form of the CRT?
THE CHINESE REMAINDER THEOREM, SO WHAT?

We can trade big $+$s and $\times$s for small(er) $+$s and $\times$s.

**EXAMPLE**

\[
\begin{array}{c|c|c|c}
  m_1 &= 5 & n_1 &= 65/5 = 13 \\
  m_2 &= 13 & n_2 &= 65/13 = 5 \\
  M &= 65 & c_1 &= n_1 \cdot (n_1^{-1} \mod m_1) = 13 \cdot 2 = 26 \\
  & & c_2 &= n_2 \cdot (n_2^{-1} \mod m_2) = 5 \cdot 8 = 40 \\
\end{array}
\]

Consider $42 +_{65} 29$.

**Computation 1**

\[42 + 29 = 71 \equiv 6 \pmod{65}.
\]

**Computation 2**

\[42 +_{64} 29 \xrightarrow{f} (2, 3) + (4, 3) = (1, 6) \xrightarrow{f^{-1}} 6.
\]

\[c_1 \cdot 1 + c_2 \cdot 6 = 26 \cdot 1 + 40 \cdot 6 = 266 \equiv 6 \pmod{65}
\]