CS70 Fall 2013
Discrete Math and Probability Theory

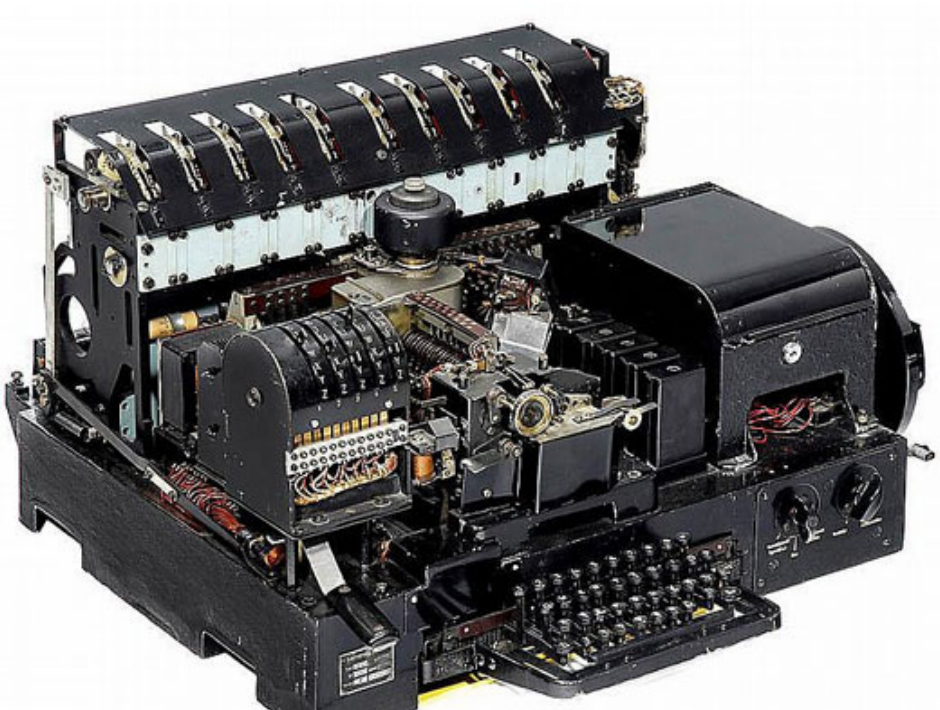
Umesh V. Vazirani
U.C. Berkeley

Lecture 7: Bijections & RSA

$$E[\underline{4024007119763398}] = \underline{1902464973302875}$$

Amazon or Ebay

A major factor in the success of the Allies from the second half of 1941 onwards was the cracking of the Enigma machine.



E[4024007119763398] = 1902464973302875

Amazon or Ebay

Rivest, Shamir
Adleman.

$N = P \cdot Q$

$P = 3 \quad Q = 5$

$$E(x) = x^e \pmod{N}.$$

$\underline{e = 3}$

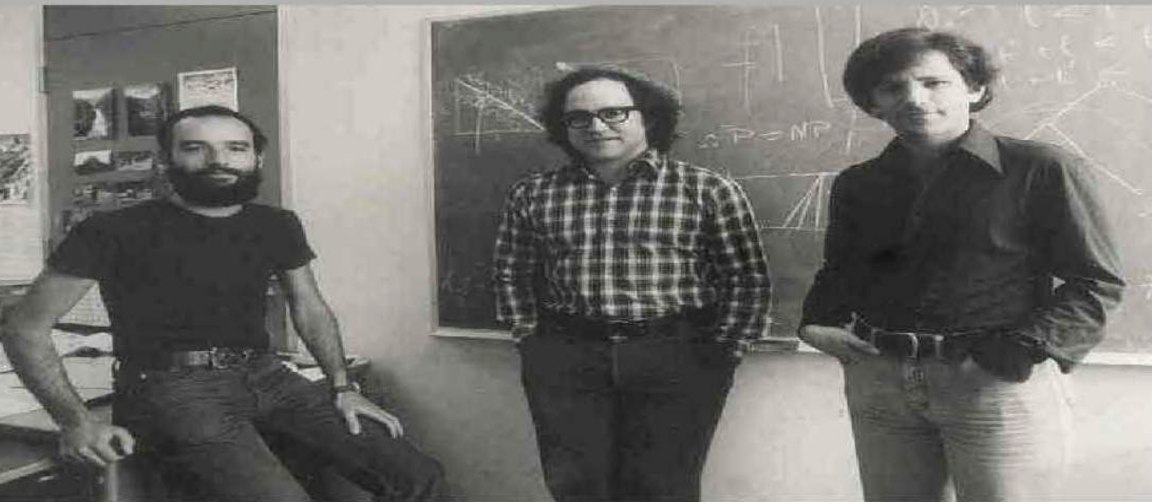
$\boxed{(N, e)} = (15, 3)$

$x = 2$

$2^3 \pmod{15} = 8$

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQCkblMUCt4s42BVmvJCpq9HEi8Xzvq63E5jVjS5unNLeEQ9xmxp
pCWzYQKdCQQ/cj3YJ9OwWkV3tzbkJiPMEriu3qe2OoI8fCRZCviWQ4ujKTY/kX9d
xyOUKX8Kzgq9jZsvGReq1Y7sZqI36z9XUzzyqrt5GUuQfqejmf6ETInwPQIDAQAB
Ffkdrei8gjoaioxaj47afajk38aladld9685rCX7ZtQEkx4qPDlqqBMMGVW/8Q34
hugrap+BIgSTzHcLB6I4DwiksUpR08x0hf0oxqqjMo0KykhZDfUUfxR85JHUrFZM
GznurVhfSBXX4Il9Tgc/RPzD32FZ6gaz9sFumJh0LKKadeECQQDWOfP6+nIAvmyH
aRINErBSlK+xvfjkjie94kfjkq9pyNyoOStYLG/DRPlEzAIA6oQnowGgS6gwaibg
g7yVTgBpAkEAxH6dcwhIDRTILvtUdKSWB6vdhtXFGdebaU4cuUOW2kWwPpyIj4XN
D+rezwfptmeOr34DCA/QKCI/BWkbFDG2tQJAVAH971nvAuOp46AMeBvwETJFg8qw
Oqw81x02X6TMEEm4Xi+tE7K5UTXnGld2Ia3VjUWbCaUhm3rFLB39Af/IoQJAUn/G
o5GKjtN26SLk5sRjqXzjWcVPJ/Z6bdA6Bx71q1cvFFqsi3XmDxTRz6LG4arBIbWK
dhjfuey7395oroC7MQJAYTfwPZ8/4x/USmA4vx9FKdADdDoZnA9ZSwezWaqa44My
bJ0SY/WmNU+Z4ldVIkcevwwwcxqLF399hjrXWhzlBQ==
-----END RSA PRIVATE KEY-----
```

IN RSA WE TRUST



$N = 15$

$(15, \underset{e}{3})$ Public key

(N, d) Private key

$N = 15$, $d = 3$.

$D(E(x)) = x$

$E(x) = x^e \pmod{N}$.

$D(y) = y^d \pmod{N}$.

$\equiv x$

$D = E^{-1}$

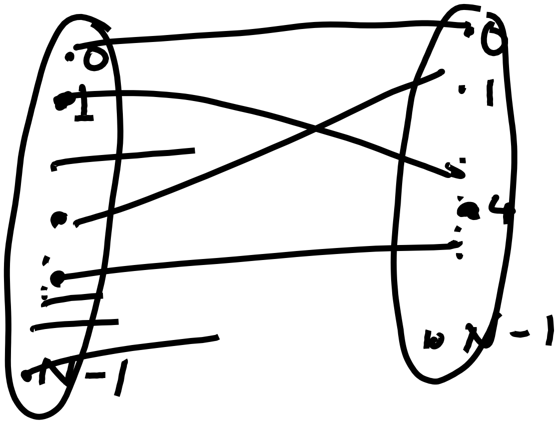
$y = 8$

$8^3 \pmod{15}$

$8 \cdot 8 \cdot 8 \pmod{15}$

$4 \cdot 8 \bmod 15 = 2$

f :



A	B
Domain	Range

X

not 1-1.

1-1

not onto.

f X $\longrightarrow$ Y

$g = f^{-1}$

$f(x=y)$

$g(y) = x$

onto

not 1-1

1-1

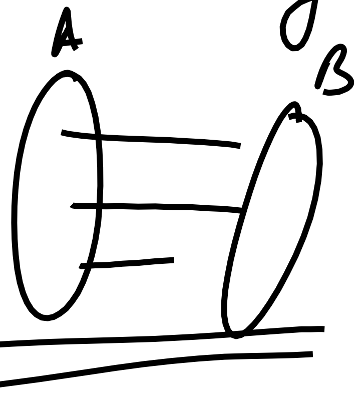
onto $\longleftrightarrow$ bijection.

One way to show that f is a bijection is to show

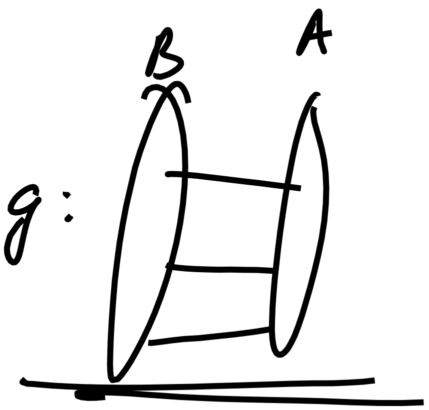
$\exists\, g : \quad g(f(x)) = x \quad \forall\, x \in A.$

$g(y)$ defined $\forall\, y \in B.$

$f :$



$g :$



$f : A \rightarrow B$

$g : B \rightarrow A.$

mod m

$59 \equiv 3 \pmod 7$

$59 = 7 \times 8 + \underline{\underline{3}}$

$+, -, \underline{\underline{\times}}$

$3^2 \pmod 7 = 2$

$3^4 \pmod 7$

$= 3^2 \times 3^2 = 4 \pmod 7$

$= \underline{\underline{3^6}} = 3^2 \times 3^2 \times 3^2 = 8$

$= 1 \pmod 7$

$3^{50} \pmod 7$

$= 3^{48+2} \pmod 7$

$= 3^{6 \times 8 + 2} \pmod 7$

$= (3^6)^8 \cdot 3^2 \pmod 7$

$= 2 \pmod 7$

0
1
2
3
4
5
6

Divisim: Division $\longleftrightarrow$ Multiplication

$$\boxed{a \cdot b = c \qquad\qquad a = \frac{c}{b}}$$

$$4 = 3 \times 6 \pmod 7 \qquad\qquad 3 = \frac{4}{6} \pmod 7$$

$$1 = 3 \times 5 \pmod 7 \qquad\qquad 3 = \frac{1}{5} \pmod 7$$

Divide by $a \pmod m$

Find x : $ax = 1 \pmod m$

$\left(a^{-1} = x = \frac{1}{a}\right) \pmod m$

$ax - 1 = my$

$ax - my = 1$

Extended Euclid : $\gcd(a, b) = 1$

$\iff \exists\, x, y : a\underline{x} + b\,\underline{y} = 1.$

$\gcd(a, m)$

$a\underline{x} + my = 1.$

$x = a^{-1}$

$a = 4$ $\quad m = 15$ $\quad \gcd(4, 15) = 1.$

$$4 \cdot x + 15y = 1.$$

$$x = 4, \quad y = -1$$

$$\frac{1}{4} \bmod 15 = 4$$

$a = 8$ $\quad m = 15$

$$8x + 15y = 1$$

$$x = 2, \quad y = -1.$$

$$8^{-1} = \frac{1}{8} \bmod 15 = 2$$

$\gcd(47, 20)$

$$47 = \underline{20} \times 2 + \underline{7}$$
$$20 = 7 \times 2 + 6$$
$$7 = \underline{6} \times 1 + 1$$
$$6 = 1 \times 6 + 0$$

$$\begin{aligned} &\gcd(47, 20) \\ &= \gcd(27, 20) \\ &= \gcd(7, 20) \\ &= \gcd(7, 13) \end{aligned}$$

Fermat’s Last Theorem

No positive integers a, b, c satisfy $a^n + b^n = c^n$ for $n > 2$.

Around 1637, Fermat wrote his Last Theorem in the margin of his
Copy of Diophantus’ Arithmetica:
it is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.

Andrew Wiles 1995.

Theorem 6.1: **[Fermat's Little Theorem]** For any prime p and any $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} = 1 \bmod p$.

$a^{(p-1)k} \equiv 1 \pmod{p}$ $\quad \forall a \quad$ $a^p = a \pmod{p}$

$p = 11$ $\quad$ $a^{(p-1)k+1} = a \pmod{p}$

$a = 3$ $\quad$ $1 = 3^{10} \pmod{11}$

$-2 = 3^2 = 9$ $\quad$ $-2 \times 3 = -6 = 3^3$

$1 = 12 = -6 \times -2 = 3^3 \times 3^2 = 3^5$

$1 = 3^{10} \pmod{11}$

$1 = 3^{10 \times 5} \pmod{11}$

$= (3^{10})^5$

$1 = (3^5)^2 = 3^5 \times 3^5$

Theorem: $N = P \cdot Q$ odd primes.

$\forall a \quad a^{(P-1)(Q-1)K+1} = a \pmod N$

Amazon (N, d) private key.

P, Q

$(P-1)(Q-1)$

You

(N, e) public key.

pick e : $\underline{\gcd(\overset{3}{\overset{\shortparallel}{e}}, (P-1)(Q-1)) = 1}$.

e has an inverse mod $(P-1)(Q-1)$

$de = 1 \mod ((P-1)(Q-1))$

$D(E(x)) = (x^{e})^{d} \mod N = x^{de} = x^{1+(P-1)(Q-1)K} = x.$

$3^6 \equiv 1 \pmod 7$

$\underline{\underline{6 = 7-1}}$

$1 \times 2 \times 3 \times 4 \times 5 \times 6$

$= (1\cdot 3)(2\cdot 3)(3\cdot 3)(4\cdot 3)(5\cdot 3)(6\cdot 3)$

$\Leftrightarrow \cancel{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6}$

$= 3^6 \cdot \cancel{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6}$

$\Leftrightarrow 3^6 = 1 \pmod 7$

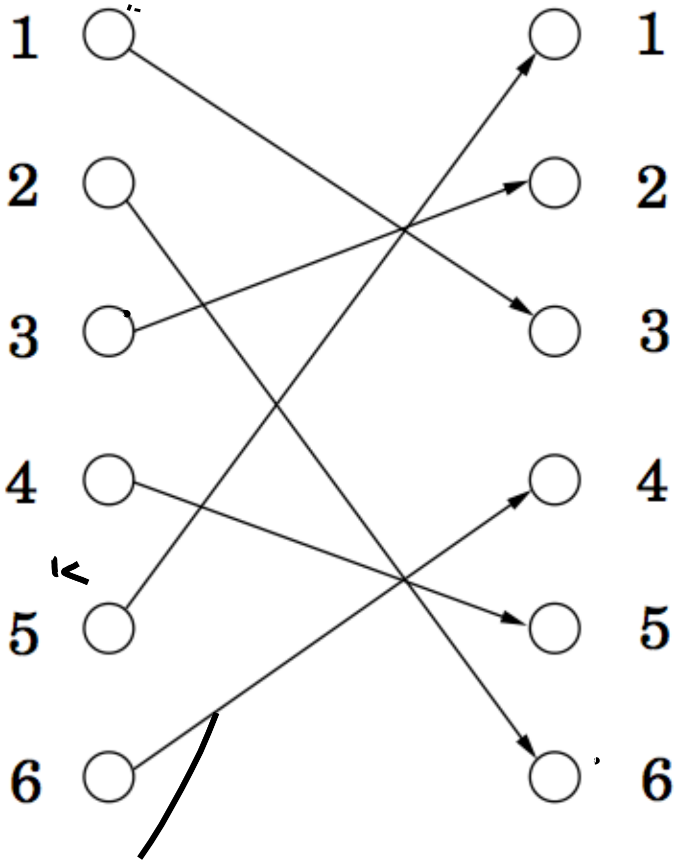


Figure 1: Multiplication by (3 mod 7)

$\times 3$ is a bijection

$\boxed{\begin{array}{l} \underline{\underline{a = 3}} \quad p = 7 \\ ja = ka \pmod p \\ \underline{\underline{(j-k)}}\, a = 0 \pmod p \end{array}}$

$\Downarrow$

$p \mid (j-k)a$