# A Taste of Cryptography and Number Theory

Jonathan H. Manton

Department of Information Engineering
Research School of Information Sciences and Engineering
The Australian National University

ANU College
2 May 2006

# Outline

# Is Mathematics Interesting?

- The Clay Mathematics Institute in the USA has set aside $7 million in prize money.

# Is Mathematics Interesting?

- The Clay Mathematics Institute in the USA has set aside $7 million in prize money.
- If anyone solves one of the seven Millenium Problems they will receive $1 million.
    1. P vs NP
    2. Riemann Hypothesis
    3. Navier-Stokes Equations
    4. Quantum Yang-Mills Theory
    5. Hodge Conjecture
    6. Poincaré Conjecture
    7. Birch and Swinnerton-Dwyer Conjecture
- In fact, one of them has (most likely) been solved...

# The RSA Algorithm in a Nutshell

- $n = pq$ where $p, q$ are distinct primes;
- $m = (p-1)(q-1)$;
- $e$ such that $\gcd(e, m) = 1$;
- $C = W^e \mod n$;
- $D = C^d \mod n$ where $ed = 1 \mod m$.

# The RSA Algorithm in a Nutshell

- $n = pq$ where $p, q$ are distinct primes;
- $m = (p-1)(q-1)$;
- $e$ such that $\gcd(e, m) = 1$;
- $C = W^e \mod n$;
- $D = C^d \mod n$ where $ed = 1 \mod m$.
- Does it work?

# The RSA Algorithm in a Nutshell

- $n = pq$ where $p, q$ are distinct primes;
- $m = (p-1)(q-1)$;
- $e$ such that $\gcd(e, m) = 1$;
- $C = W^e \mod n$;
- $D = C^d \mod n$ where $ed = 1 \mod m$.
- Does it work?
- Does $D = W$ always?

# The RSA Algorithm in a Nutshell

- $n = pq$ where $p, q$ are distinct primes;
- $m = (p-1)(q-1)$;
- $e$ such that $\gcd(e, m) = 1$;
- $C = W^e \mod n$;
- $D = C^d \mod n$ where $ed = 1 \mod m$.
- Does it work?
- Does $D = W$ always? Note that:

$$\begin{aligned} D &= C^d \mod n \\ &= (W^e)^d \mod n \\ &= W^{ed} \mod n. \end{aligned}$$

# The RSA Algorithm in a Nutshell

- $n = pq$ where $p, q$ are distinct primes;
- $m = (p-1)(q-1)$;
- $e$ such that $\gcd(e, m) = 1$;
- $C = W^e \mod n$;
- $D = C^d \mod n$ where $ed = 1 \mod m$.
- Does it work?
- Does $D = W$ always? Note that:

$$\begin{aligned} D &= C^d \mod n \\ &= (W^e)^d \mod n \\ &= W^{ed} \mod n. \end{aligned}$$

- Does $W^{ed} - W = 0 \mod n$?

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$,

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$, if $ed = 1 \mod (p-1)(q-1)$

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$, if $ed = 1 \mod (p-1)(q-1)$ then $W^{ed} - W = 0 \mod pq$.

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$, if $ed = 1 \mod (p-1)(q-1)$ then $W^{ed} - W = 0 \mod pq$.
- Proofs are easier to check than to derive!

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$, if $ed = 1 \mod (p-1)(q-1)$ then $W^{ed} - W = 0 \mod pq$.
- Proofs are easier to check than to derive! Usually, will only begin to understand a proof if you write it out yourself.

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$, if $ed = 1 \mod (p-1)(q-1)$ then $W^{ed} - W = 0 \mod pq$.
- Proofs are easier to check than to derive! Usually, will only begin to understand a proof if you write it out yourself.
- We will need two facts. (Break something complicated up into little parts, understand the parts well.)

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$, if $ed = 1 \mod (p-1)(q-1)$ then $W^{ed} - W = 0 \mod pq$.
- Proofs are easier to check than to derive! Usually, will only begin to understand a proof if you write it out yourself.
- We will need two facts. (Break something complicated up into little parts, understand the parts well.)
- Fact 1 (Fermat's Little Theorem): If $p$ is prime

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$, if $ed = 1 \mod (p-1)(q-1)$ then $W^{ed} - W = 0 \mod pq$.
- Proofs are easier to check than to derive! Usually, will only begin to understand a proof if you write it out yourself.
- We will need two facts. (Break something complicated up into little parts, understand the parts well.)
- Fact 1 (Fermat's Little Theorem): If $p$ is prime and $a \neq 0 \mod p$

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$, if $ed = 1 \mod (p-1)(q-1)$ then $W^{ed} - W = 0 \mod pq$.
- Proofs are easier to check than to derive! Usually, will only begin to understand a proof if you write it out yourself.
- We will need two facts. (Break something complicated up into little parts, understand the parts well.)
- Fact 1 (Fermat's Little Theorem): If $p$ is prime and $a \neq 0 \mod p$ then $a^{p-1} = 1 \mod p$.

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$, if $ed = 1 \mod (p-1)(q-1)$ then $W^{ed} - W = 0 \mod pq$.
- Proofs are easier to check than to derive! Usually, will only begin to understand a proof if you write it out yourself.
- We will need two facts. (Break something complicated up into little parts, understand the parts well.)
- Fact 1 (Fermat's Little Theorem): If $p$ is prime and $a \neq 0 \mod p$ then $a^{p-1} = 1 \mod p$. (If $a = 0 \mod p$ then $a^{p-1} = 0 \mod p$.)

# Does it Work? (I)

- Recall $n = pq$, $m = (p-1)(q-1)$.
- Thus, we must prove that for any $W \in \{0, \cdots, n-1\}$, if $ed = 1 \mod (p-1)(q-1)$ then $W^{ed} - W = 0 \mod pq$.
- Proofs are easier to check than to derive! Usually, will only begin to understand a proof if you write it out yourself.
- We will need two facts. (Break something complicated up into little parts, understand the parts well.)
- Fact 1 (Fermat's Little Theorem): If $p$ is prime and $a \neq 0 \mod p$ then $a^{p-1} = 1 \mod p$. (If $a = 0 \mod p$ then $a^{p-1} = 0 \mod p$.)
- Example, mod 5: $1^4 = 1$, $2^4 = 16 \equiv 1$, $3^4 = 81 \equiv 1$, $4^4 = 256 \equiv 1$.

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$,

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Example ($p = 2$, $q = 3$):

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| mod 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| mod 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| mod 6 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 0 |

- Proof:

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Example ($p = 2$, $q = 3$):

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| mod 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| mod 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| mod 6 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 0 |

- Proof: If $x = 0 \mod p$ then $x = pn$ for some integer $n$.

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Example ($p = 2$, $q = 3$):

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| mod 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| mod 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| mod 6 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 0 |

- Proof: If $x = 0 \mod p$ then $x = pn$ for some integer $n$. Similarly, we know $x = qm$ for some integer $m$.
- What values of $m$ and $n$ are possible if $pn = qm$?

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Example ($p = 2$, $q = 3$):

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| mod 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| mod 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| mod 6 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 0 |

- Proof: If $x = 0 \mod p$ then $x = pn$ for some integer $n$. Similarly, we know $x = qm$ for some integer $m$.
- What values of $m$ and $n$ are possible if $pn = qm$?
- Example: $2n = 3m$.

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Example ($p = 2$, $q = 3$):

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| mod 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| mod 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| mod 6 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 0 |

- Proof: If $x = 0 \mod p$ then $x = pn$ for some integer $n$. Similarly, we know $x = qm$ for some integer $m$.
- What values of $m$ and $n$ are possible if $pn = qm$?
- Example: $2n = 3m$. Then $m = \frac{2n}{3}$.

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Example ($p = 2$, $q = 3$):

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| mod 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| mod 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| mod 6 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 0 |

- Proof: If $x = 0 \mod p$ then $x = pn$ for some integer $n$. Similarly, we know $x = qm$ for some integer $m$.
- What values of $m$ and $n$ are possible if $pn = qm$?
- Example: $2n = 3m$. Then $m = \frac{2n}{3}$. So $n = 1$ does not work.

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Example ($p = 2$, $q = 3$):

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| mod 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| mod 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| mod 6 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 0 |

- Proof: If $x = 0 \mod p$ then $x = pn$ for some integer $n$. Similarly, we know $x = qm$ for some integer $m$.
- What values of $m$ and $n$ are possible if $pn = qm$?
- Example: $2n = 3m$. Then $m = \frac{2n}{3}$. So $n = 1$ does not work. Nor does $n = 2$.

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Example ($p = 2$, $q = 3$):

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| mod 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| mod 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| mod 6 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 0 |

- Proof: If $x = 0 \mod p$ then $x = pn$ for some integer $n$. Similarly, we know $x = qm$ for some integer $m$.
- What values of $m$ and $n$ are possible if $pn = qm$?
- Example: $2n = 3m$. Then $m = \frac{2n}{3}$. So $n = 1$ does not work. Nor does $n = 2$. But $n = 3$ works.

# Does it Work? (II)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Example ($p = 2$, $q = 3$):

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| mod 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| mod 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| mod 6 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 0 |

- Proof: If $x = 0 \mod p$ then $x = pn$ for some integer $n$. Similarly, we know $x = qm$ for some integer $m$.
- What values of $m$ and $n$ are possible if $pn = qm$?
- Example: $2n = 3m$. Then $m = \frac{2n}{3}$. So $n = 1$ does not work. Nor does $n = 2$. But $n = 3$ works.
- There is a solution only if $n$ is divisible by 3.

# Does it Work? (III)

- Fact 2: If $p$ and $q$ are distinct primes

# Does it Work? (III)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$,

# Does it Work? (III)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Proof: We know $x = pn$ and $x = qm$. Therefore $pn = qm$.

# Does it Work? (III)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Proof: We know $x = pn$ and $x = qm$. Therefore $pn = qm$.
- Therefore $qm$ must be divisible by $p$.

# Does it Work? (III)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Proof: We know $x = pn$ and $x = qm$. Therefore $pn = qm$.
- Therefore $qm$ must be divisible by $p$. $\left(n = \frac{qm}{p}\right)$.

# Does it Work? (III)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Proof: We know $x = pn$ and $x = qm$. Therefore $pn = qm$.
- Therefore $qm$ must be divisible by $p$. $\left(n = \frac{qm}{p}\right)$.
- Since $p$ is prime, we have learnt this means either $q$ is divisible by $p$ or $m$ is divisible by $p$. The former cannot happen since $q$ is a prime different from $p$.

# Does it Work? (III)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Proof: We know $x = pn$ and $x = qm$. Therefore $pn = qm$.
- Therefore $qm$ must be divisible by $p$. $\left(n = \frac{qm}{p}\right)$.
- Since $p$ is prime, we have learnt this means either $q$ is divisible by $p$ or $m$ is divisible by $p$. The former cannot happen since $q$ is a prime different from $p$.
- Thus, $m = pk$ for some integer $k$.

# Does it Work? (III)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Proof: We know $x = pn$ and $x = qm$. Therefore $pn = qm$.
- Therefore $qm$ must be divisible by $p$. $\left(n = \frac{qm}{p}\right)$.
- Since $p$ is prime, we have learnt this means either $q$ is divisible by $p$ or $m$ is divisible by $p$. The former cannot happen since $q$ is a prime different from $p$.
- Thus, $m = pk$ for some integer $k$.
- Thus, $x = qm = qpk = (pq)k$.

# Does it Work? (III)

- Fact 2: If $p$ and $q$ are distinct primes and if $x = 0 \mod p$, and $x = 0 \mod q$, then $x = 0 \mod pq$.
- Proof: We know $x = pn$ and $x = qm$. Therefore $pn = qm$.
- Therefore $qm$ must be divisible by $p$. $\left(n = \frac{qm}{p}\right)$.
- Since $p$ is prime, we have learnt this means either $q$ is divisible by $p$ or $m$ is divisible by $p$. The former cannot happen since $q$ is a prime different from $p$.
- Thus, $m = pk$ for some integer $k$.
- Thus, $x = qm = qpk = (pq)k$. In other words, $x = 0 \mod pq$, as required.

# Does it Work? (IV)

- If $ed = 1 \mod (p-1)(q-1)$, prove $W^{ed} - W = 0 \mod pq$.

# Does it Work? (IV)

- If $ed = 1 \mod (p-1)(q-1)$, prove $W^{ed} - W = 0 \mod pq$.
- By Fact 2, it suffices to show $W^{ed} - W = 0 \mod p$ and $W^{ed} - W = 0 \mod q$.

# Does it Work? (IV)

- If $ed = 1 \mod (p-1)(q-1)$, prove $W^{ed} - W = 0 \mod pq$.
- By Fact 2, it suffices to show $W^{ed} - W = 0 \mod p$ and $W^{ed} - W = 0 \mod q$.
- Since the roles of $p$ and $q$ are the same, if we prove $W^{ed} - W = 0 \mod p$ then we know $W^{ed} - W = 0 \mod q$ too.

# Does it Work? (IV)

- If $ed = 1 \mod (p-1)(q-1)$, prove $W^{ed} - W = 0 \mod pq$.
- By Fact 2, it suffices to show $W^{ed} - W = 0 \mod p$ and $W^{ed} - W = 0 \mod q$.
- Since the roles of $p$ and $q$ are the same, if we prove $W^{ed} - W = 0 \mod p$ then we know $W^{ed} - W = 0 \mod q$ too.
- Note that $ed = 1 + (p-1)(q-1)k$ for some integer $k$.

# Does it Work? (IV)

- If $ed = 1 \mod (p-1)(q-1)$, prove $W^{ed} - W = 0 \mod pq$.
- By Fact 2, it suffices to show $W^{ed} - W = 0 \mod p$ and $W^{ed} - W = 0 \mod q$.
- Since the roles of $p$ and $q$ are the same, if we prove $W^{ed} - W = 0 \mod p$ then we know $W^{ed} - W = 0 \mod q$ too.
- Note that $ed = 1 + (p-1)(q-1)k$ for some integer $k$.

$$\begin{aligned} W^{ed} - W &= W^{1+(p-1)(q-1)k} - W \\ &= W\left(W^{(p-1)(q-1)k} - 1\right) \end{aligned}$$

# Does it Work? (V)

- Does $W\left(W^{(p-1)(q-1)k} - 1\right) = 0 \mod p$?

# Does it Work? (V)

- Does $W\left(W^{(p-1)(q-1)k} - 1\right) = 0 \mod p$?
- Case 1: If $W \mod p = 0$, then yes!

# Does it Work? (V)

- Does $W\left(W^{(p-1)(q-1)k} - 1\right) = 0 \mod p$?
- Case 1: If $W \mod p = 0$, then yes!
- Case 2: If $W \mod p \neq 0$, then we know from Fermat's Little Theorem that $W^{p-1} = 1 \mod p$.

# Does it Work? (V)

- Does $W\left(W^{(p-1)(q-1)k} - 1\right) = 0 \mod p$?
- Case 1: If $W \mod p = 0$, then yes!
- Case 2: If $W \mod p \neq 0$, then we know from Fermat's Little Theorem that $W^{p-1} = 1 \mod p$.
- Observe that $W^{(p-1)(q-1)k} = \left\{W^{(p-1)}\right\}^{(q-1)k}$.

# Does it Work? (V)

- Does $W\left(W^{(p-1)(q-1)k}-1\right)=0 \mod p$?
- Case 1: If $W \mod p=0$, then yes!
- Case 2: If $W \mod p \neq 0$, then we know from Fermat's Little Theorem that $W^{p-1}=1 \mod p$.
- Observe that $W^{(p-1)(q-1)k}=\left\{W^{(p-1)}\right\}^{(q-1)k}$.
- Hence, $\mod p$, we have

$$\begin{aligned}
W\left(W^{(p-1)(q-1)k}-1\right) &\equiv W\left(\left\{W^{(p-1)}\right\}^{(q-1)k}-1\right) \\
&\equiv W\left(1^{(q-1)k}-1\right) \\
&\equiv W(1-1) \\
&\equiv 0
\end{aligned}$$

# Is it Secure?

- Given $W^e \mod n$, can we work out what $W$ is?

# Is it Secure?

- Given $W^e \mod n$, can we work out what $W$ is?
- We know $e$ and $n$.
- However, only two known methods for recovering $W$.
    1. Trial and error; guess $W$.

# Is it Secure?

- Given $W^e \mod n$, can we work out what $W$ is?
- We know $e$ and $n$.
- However, only two known methods for recovering $W$.
  1. Trial and error; guess $W$.
  2. Figure out $p$ and $q$ where $n = pq$.

# Is it Secure?

- Given $W^e \mod n$, can we work out what $W$ is?
- We know $e$ and $n$.
- However, only two known methods for recovering $W$.
  1. Trial and error; guess $W$.
  2. Figure out $p$ and $q$ where $n = pq$.
- The second option is much faster, hence the security of RSA appears to rest on our inability to factor large numbers.
- RSA would be "provably secure" if we can prove:
  1. The fastest way of finding $W$ given $W^e \mod n$ is to factor $n$.

# Is it Secure?

- Given $W^e \mod n$, can we work out what $W$ is?
- We know $e$ and $n$.
- However, only two known methods for recovering $W$.
  1. Trial and error; guess $W$.
  2. Figure out $p$ and $q$ where $n = pq$.
- The second option is much faster, hence the security of RSA appears to rest on our inability to factor large numbers.
- RSA would be "provably secure" if we can prove:
  1. The fastest way of finding $W$ given $W^e \mod n$ is to factor $n$.
  2. Factoring large numbers cannot be done quickly.
- How could we possibly (hope to) prove either of these?

# Equal Difficulty

- What does it mean for Problem A to be equally difficult as Problem B?

# Equal Difficulty

- What does it mean for Problem A to be equally difficult as Problem B?
- Breaking RSA equally difficult as factoring large numbers?

# Equal Difficulty

- What does it mean for Problem A to be equally difficult as Problem B?
- Breaking RSA equally difficult as factoring large numbers?
- We know that if we can factor large numbers, we can break RSA.

# Equal Difficulty

- What does it mean for Problem A to be equally difficult as Problem B?
- Breaking RSA equally difficult as factoring large numbers?
- We know that if we can factor large numbers, we can break RSA.
- Hence, RSA is no more difficult than factoring large numbers.

# Equal Difficulty

- What does it mean for Problem A to be equally difficult as Problem B?
- Breaking RSA equally difficult as factoring large numbers?
- We know that if we can factor large numbers, we can break RSA.
- Hence, RSA is no more difficult than factoring large numbers.
- One way to prove the converse is to prove that if we can break RSA quickly, we can factor large numbers quickly!

# Equal Difficulty

- What does it mean for Problem A to be equally difficult as Problem B?
- Breaking RSA equally difficult as factoring large numbers?
- We know that if we can factor large numbers, we can break RSA.
- Hence, RSA is no more difficult than factoring large numbers.
- One way to prove the converse is to prove that if we can break RSA quickly, we can factor large numbers quickly!
- Rough idea: For any $e$ and $n$, we assume that given $W^e \bmod n$ we can quickly find $W$. Given this “new operation”, can we now factor large numbers quickly?

# Equal Difficulty

- What does it mean for Problem A to be equally difficult as Problem B?
- Breaking RSA equally difficult as factoring large numbers?
- We know that if we can factor large numbers, we can break RSA.
- Hence, RSA is no more difficult than factoring large numbers.
- One way to prove the converse is to prove that if we can break RSA quickly, we can factor large numbers quickly!
- Rough idea: For any $e$ and $n$, we assume that given $W^e \bmod n$ we can quickly find $W$. Given this “new operation”, can we now factor large numbers quickly?
- Area of Mathematics: Computational Complexity Theory

# Factoring Large Numbers

- We currently think factoring large numbers is difficult. But why should anything be difficult?

# Factoring Large Numbers

- We currently think factoring large numbers is difficult. But why should anything be difficult?
- Roughly speaking, there are only so many different computer programs we can write. (Finite memory, finite processing speed, a useful program must terminate within a reasonable time.)

# Factoring Large Numbers

- We currently think factoring large numbers is difficult. But why should anything be difficult?
- Roughly speaking, there are only so many different computer programs we can write. (Finite memory, finite processing speed, a useful program must terminate within a reasonable time.)
- The number of problems out there exceeds the number of computer programs!

# Factoring Large Numbers

- We currently think factoring large numbers is difficult. But why should anything be difficult?
- Roughly speaking, there are only so many different computer programs we can write. (Finite memory, finite processing speed, a useful program must terminate within a reasonable time.)
- The number of problems out there exceeds the number of computer programs!
- Therefore, we believe that there are difficult problems out there. We just don't know very much about which problems are difficult. (Does P equal NP?)

# Factoring Large Numbers

- We currently think factoring large numbers is difficult. But why should anything be difficult?
- Roughly speaking, there are only so many different computer programs we can write. (Finite memory, finite processing speed, a useful program must terminate within a reasonable time.)
- The number of problems out there exceeds the number of computer programs!
- Therefore, we believe that there are difficult problems out there. We just don't know very much about which problems are difficult. (Does P equal NP?)
- Note that most research has been based around "computers" which add and multiply numbers.

# Factoring Large Numbers

- We currently think factoring large numbers is difficult. But why should anything be difficult?
- Roughly speaking, there are only so many different computer programs we can write. (Finite memory, finite processing speed, a useful program must terminate within a reasonable time.)
- The number of problems out there exceeds the number of computer programs!
- Therefore, we believe that there are difficult problems out there. We just don't know very much about which problems are difficult. (Does P equal NP?)
- Note that most research has been based around "computers" which add and multiply numbers.
- Is there any other kind of computer?

# Factoring Large Numbers

- We currently think factoring large numbers is difficult. But why should anything be difficult?
- Roughly speaking, there are only so many different computer programs we can write. (Finite memory, finite processing speed, a useful program must terminate within a reasonable time.)
- The number of problems out there exceeds the number of computer programs!
- Therefore, we believe that there are difficult problems out there. We just don't know very much about which problems are difficult. (Does P equal NP?)
- Note that most research has been based around "computers" which add and multiply numbers.
- Is there any other kind of computer?
- What would it mean for the security of RSA?

# Quantum Computers

- We live in a quantum mechanical world.

# Quantum Computers

- We live in a quantum mechanical world.
- If we could build computers which did not add and subtract, but rather performed “quantum mechanical operations”, things that were hard on ordinary computers might become easy, and vice versa.

# Quantum Computers

- We live in a quantum mechanical world.
- If we could build computers which did not add and subtract, but rather performed “quantum mechanical operations”, things that were hard on ordinary computers might become easy, and vice versa.
- In fact, the great strength of quantum computers is that they can perform the same operation on a large amount of data simultaneously.

# Quantum Computers

- We live in a quantum mechanical world.
- If we could build computers which did not add and subtract, but rather performed “quantum mechanical operations”, things that were hard on ordinary computers might become easy, and vice versa.
- In fact, the great strength of quantum computers is that they can perform the same operation on a large amount of data simultaneously.
- Roughly speaking, we can break RSA using a quantum computer by trial and error because we can guess a very large number of solutions in one operation.

# Quantum Computers

- We live in a quantum mechanical world.
- If we could build computers which did not add and subtract, but rather performed “quantum mechanical operations”, things that were hard on ordinary computers might become easy, and vice versa.
- In fact, the great strength of quantum computers is that they can perform the same operation on a large amount of data simultaneously.
- Roughly speaking, we can break RSA using a quantum computer by trial and error because we can guess a very large number of solutions in one operation.
- This words because the speed-up does not grow with $N$ but with $2^N$; if $N$ is the size of the quantum computer, then we can check around $2^N$ possible solutions per operation. (At least, something like this is true.)

# Who Wrote the Email?

- Wilma receives an email purportedly from Fred.

# Who Wrote the Email?

- Wilma receives an email purportedly from Fred.
- Did Fred or Charlie send the email though?

# Who Wrote the Email?

- Wilma receives an email purportedly from Fred.
- Did Fred or Charlie send the email though?
- What scheme can we think of that would allow Wilma to be sure that Fred wrote the email?

# Who Wrote the Email?

- Wilma receives an email purportedly from Fred.
- Did Fred or Charlie send the email though?
- What scheme can we think of that would allow Wilma to be sure that Fred wrote the email?
- In RSA, encryption easy, decryption hard.

# Who Wrote the Email?

- Wilma receives an email purportedly from Fred.
- Did Fred or Charlie send the email though?
- What scheme can we think of that would allow Wilma to be sure that Fred wrote the email?
- In RSA, encryption easy, decryption hard.
- Idea: Reverse the roles! Make encryption hard, and decryption easy!

# Who Wrote the Email?

- Wilma receives an email purportedly from Fred.
- Did Fred or Charlie send the email though?
- What scheme can we think of that would allow Wilma to be sure that Fred wrote the email?
- In RSA, encryption easy, decryption hard.
- Idea: Reverse the roles! Make encryption hard, and decryption easy!
- That is, we encode using the private key, and decode using the public key.

# Who Wrote the Email?

- Wilma receives an email purportedly from Fred.
- Did Fred or Charlie send the email though?
- What scheme can we think of that would allow Wilma to be sure that Fred wrote the email?
- In RSA, encryption easy, decryption hard.
- Idea: Reverse the roles! Make encryption hard, and decryption easy!
- That is, we encode using the private key, and decode using the public key.
- Only Fred knows his own private key, hence only Fred can encode his email using his private key.

# Who Wrote the Email?

- Wilma receives an email purportedly from Fred.
- Did Fred or Charlie send the email though?
- What scheme can we think of that would allow Wilma to be sure that Fred wrote the email?
- In RSA, encryption easy, decryption hard.
- Idea: Reverse the roles! Make encryption hard, and decryption easy!
- That is, we encode using the private key, and decode using the public key.
- Only Fred knows his own private key, hence only Fred can encode his email using his private key.
- Everyone can decode Fred's email using his public key.

# Who Wrote the Email?

- Wilma receives an email purportedly from Fred.
- Did Fred or Charlie send the email though?
- What scheme can we think of that would allow Wilma to be sure that Fred wrote the email?
- In RSA, encryption easy, decryption hard.
- Idea: Reverse the roles! Make encryption hard, and decryption easy!
- That is, we encode using the private key, and decode using the public key.
- Only Fred knows his own private key, hence only Fred can encode his email using his private key.
- Everyone can decode Fred's email using his public key.
- In reality, we send the email in plaintext. We also compute a "hash" or "checksum", and encode this checksum using our private key.

# Summary and Closing Thoughts

- We proved RSA works. Required Fermat's Little Theorem and other facts from number theory.

# Summary and Closing Thoughts

- We proved RSA works. Required Fermat's Little Theorem and other facts from number theory.
- We stated the security of RSA is an open problem. Academics spend their lives working on open problems!

# Summary and Closing Thoughts

- We proved RSA works. Required Fermat's Little Theorem and other facts from number theory.
- We stated the security of RSA is an open problem. Academics spend their lives working on open problems!
- Mathematics evolves. Hard things become simple, thus becoming building blocks for even harder things.

# Summary and Closing Thoughts

- We proved RSA works. Required Fermat's Little Theorem and other facts from number theory.
- We stated the security of RSA is an open problem. Academics spend their lives working on open problems!
- Mathematics evolves. Hard things become simple, thus becoming building blocks for even harder things.
- It is the ability of mathematics to solve new and challenging problems which makes it so exciting, and its evolution is an art which can be admired in the same way paintings are admired.

# Summary and Closing Thoughts

- We proved RSA works. Required Fermat's Little Theorem and other facts from number theory.
- We stated the security of RSA is an open problem. Academics spend their lives working on open problems!
- Mathematics evolves. Hard things become simple, thus becoming building blocks for even harder things.
- It is the ability of mathematics to solve new and challenging problems which makes it so exciting, and its evolution is an art which can be admired in the same way paintings are admired.
- Usually, a considerable knowledge is required before this appreciation comes; this is the challenge of teaching mathematics!