Understanding the Magic: Teaching Cryptography with Just the Right Amount of Mathematics

Joshua Holden
Rose-Hulman Institute of Technology
http://www.rose-hulman.edu/~holden

Joint Meetings, 9 January 2004

What am I going to show you?

- Pohlig-Hellman exponentiation cipher
- Fermat's Little Theorem
- Necessary ideas for RSA
- One way to mix mathematics and cryptography
- A neat "magic trick"?

What comes before?

- Shift ciphers
- Modular arithmetic
- Multiplicative ciphers
- Euclidean algorithm and multiplicative inverses
- Block ciphers (e.g. Hill cipher)
- Private-key vs. public-key ciphers

Pohlig-Hellman exponentiation cipher (1978)

- Private key block cipher
- m letters $\rightarrow$ $2m$-digit number
- Example: $m = 2$, blocks are 4 digit numbers
  - ☐ ca $\rightarrow$ 0200
  - ☐ ts $\rightarrow$ 1918
  - ☐ an $\rightarrow$ 0013
  - ☐ dd $\rightarrow$ 0303
  - ☐ og $\rightarrow$ 1406
  - ☐ sx $\rightarrow$ 1803

Encryption

- Pick a prime number larger than the largest possible block

- e.g. $p > 2525$, say $p = 3001$

- Pick a key, e

- Shift ciphers: add key.
  Multiplicative ciphers: multiply by key.
  Exponential cipher: $C \equiv P^e \mod p$.
  (C is ciphertext block; P is plaintext block)

- Let $e = 7$, then
  - □ $(0200)^7 \equiv 1640 \mod 3001$
  - □ $(1918)^7 \equiv 0213 \mod 3001$
  - □ $(0013)^7 \equiv 0608 \mod 3001$
  - □ $(0303)^7 \equiv 1140 \mod 3001$
  - □ $(1406)^7 \equiv 2918 \mod 3001$
  - □ $(1823)^7 \equiv 0094 \mod 3001$

Decryption

- Now we have ciphertext. Recipient needs to recover plaintext P.

- Need to be able to take e-th roots!

- $C^{1/e} \mod p$ doesn't make sense.

- Need an inverse of some sort. What sort?

- Need a number d such that $C^d \equiv P \mod p$
  $\Leftrightarrow (P^e)^d \equiv P \mod p$
  $\Leftrightarrow P^{ed} \equiv P \mod p$
  $\Leftrightarrow P^{ed}P^{-1} \equiv 1 \mod p$
  $\Leftrightarrow P^{ed-1} \equiv 1 \mod p$

- So it's very important to know what numbers x have $P^x \equiv 1 \mod p$

Theorem (Fermat's Little Theorem, 1640) If p is a prime number and a is a positive integer, $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.

"Proof by Example" $3^6 \equiv 1 \mod 7$

Start with 1,2,3,4,5,6.

Multiply each by 3 mod 7: 3,6,2,5,1,4.

Second row is a rearrangement of the first!

So $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \mod 7$
$\equiv (3 \cdot 1)(3 \cdot 2)(3 \cdot 3)(3 \cdot)(3 \cdot 5)(3 \cdot 6) \mod 7$
$\equiv 3^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \mod 7.$

All of $k = 1, 2, 3, 4, 5, 6$ have $\gcd(k, 7) = 1$, so can multiply by their inverses to cancel.
Thus $1 \equiv 3^6 \mod 7$

Real Proof (if desired) (pretty much the same!)

Now what do we need to decrypt?

- Need $P^{ed-1} \equiv 1 \mod p$

- This works if $ed-1 = k(p-1)$ because then
  $P^{ed-1} \equiv P^{k(p-1)} \mod p$
  $\equiv (P^{(p-1)})^k \mod p$
  $\equiv 1^k \mod p$
  $\equiv 1 \mod p$

- $ed - 1 = k(p - 1)$ means $ed \equiv 1 \mod p - 1$
  $\Leftrightarrow d \equiv \overline{e} \mod p - 1$ (not $\mod p$!)

- So for decryption we figure out
  $d \equiv \overline{e} \mod p - 1$
  using gcd($e, p - 1$), which had better $= 1$

  and let $P \equiv C^d \equiv C^{\overline{e}} \mod p$

- Luckily, if $p = 3001$, $e = 7$, then $\gcd(7, 3000) = 1$ so we can decrypt

- $d \equiv \overline{e} \equiv 2143 \mod p - 1 = 3000$ (using the Euclidean algorithm)

  - □ $(1640)^{2143} \equiv 0200 \mod 3001 \rightarrow$ ca

  - □ $(0213)^{2143} \equiv 1918 \mod 3001 \rightarrow$ ts

  - □ $(0608)^{2143} \equiv 0013 \mod 3001 \rightarrow$ an

  - □ $(1140)^{2143} \equiv 0303 \mod 3001 \rightarrow$ dd

  - □ $(2918)^{2143} \equiv 1406 \mod 3001 \rightarrow$ og

  - □ $(0094)^{2143} \equiv 1823 \mod 3001 \rightarrow$ sx

- Magic! But now you know the trick.

What comes next?

- Security: the discrete log problem
- Exponentiation with composite moduli
- Where Fermat's Little Theorem breaks
- The Euler phi function
- Euler's Theorem
- RSA
- Fast exponentiation
- Fast primality testing
- ...