The Pohlig-Hellman exponentiation cipher as a bridge between classical and modern cryptography

Joshua Holden

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

ROSE-HULMAN INSTITUTE OF TECHNOLOGY

The Pohlig-Hellman Exponentiation Cipher: Background

- Originally proposed in 1976 (about same time as Diffie-Hellman)
- Not published until after RSA and Diffie-Hellman
- Private key cipher
- In some ways, logical successor to classical ciphers
- But also uses ideas from RSA and Diffie-Hellman

A Classical (Block) Additive 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 $\rightarrow$ 1823

Additive Encryption

- Pick a modulus *n* larger than the largest possible block
- e.g. $n > 2525$, say $n = 3000$
- Pick a key, *e*, between 1 and *n*
- Add the key to the plaintext block to get the ciphertext block

Example

- Let $e = 1640$, then
  - $0200 + 1640 \equiv 1840 \mod 3000$
  - $1918 + 1640 \equiv 0558 \mod 3000$
  - $0013 + 1640 \equiv 1653 \mod 3000$
  - $0303 + 1640 \equiv 1943 \mod 3000$
  - $1406 + 1640 \equiv 0046 \mod 3000$
  - $1823 + 1640 \equiv 0463 \mod 3000$

Additive Decryption

- Subtract the key to get the plaintext block back
  - $1840 - 1640 \equiv 0200 \mod 3000 \to$ ca
  - $0558 - 1640 \equiv 1918 \mod 3000 \to$ ts
  - $1653 - 1640 \equiv 0013 \mod 3000 \to$ an
  - $1943 - 1640 \equiv 0303 \mod 3000 \to$ dd
  - $0046 - 1640 \equiv 1406 \mod 3000 \to$ og
  - $0463 - 1640 \equiv 1823 \mod 3000 \to$ sx

Multiplicative Encryption

- A “small” variation
- Probably not used classically, but could have been
- This time the modulus and the key need to be relatively prime
- e.g. $n = 3000$, $e = 1801$
- Multiply the key by the plaintext block to get the ciphertext block
    - $0200 \times 1801 \equiv 0200 \mod 3000$
    - $1918 \times 1801 \equiv 1318 \mod 3000$
    - $0013 \times 1801 \equiv 2413 \mod 3000$
    - $0303 \times 1801 \equiv 2703 \mod 3000$
    - $1406 \times 1801 \equiv 0206 \mod 3000$
    - $1823 \times 1801 \equiv 1223 \mod 3000$

Multiplicative Decryption

- Since $\gcd(e, n) = 1$, we can use the Euclidean Algorithm to find

$$d \equiv \overline{e} \mod n$$

- In this case $\overline{1801} \equiv 1201 \mod 3000$
- Multiply the "decryption key" d by the ciphertext block to get the plaintext block
  - $0200 \times 1201 \equiv 0200 \mod 3000 \to$ca
  - $1318 \times 1201 \equiv 1918 \mod 3000 \to$ts
  - $2413 \times 1201 \equiv 0013 \mod 3000 \to$an
  - $2703 \times 1201 \equiv 0303 \mod 3000 \to$dd
  - $0206 \times 1201 \equiv 1406 \mod 3000 \to$og
  - $1223 \times 1201 \equiv 1823 \mod 3000 \to$sx

Pohlig-Hellman Encryption

- Seems like a logical extension
- Pick a prime number larger than the largest possible block
- e.g. $p > 2525$, say $p = 3001$
- Pick a key, e
- $C \equiv P^e \mod p$
- (C is ciphertext block; P is plaintext block)

Pohlig-Hellman Encryption, continued

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

Pohlig-Hellman Decryption

- Now we have ciphertext. Recipient needs to recover plaintext P.
- Need to be able to take e-th roots!
- Need an inverse of some sort again. 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 $a^{p-1} \equiv 1 \mod p$.

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

$$\begin{aligned} P^{ed-1} &\equiv P^{k(p-1)} \mod p \\ &\equiv (P^{(p-1)})^k \mod p \\ &\equiv 1^k \mod p \\ &\equiv 1 \mod p \end{aligned}$$

- $ed - 1 = k(p-1)$ means $ed \equiv 1 \mod p-1$ $\Leftrightarrow d \equiv \overline{e} \mod p-1$ (not modulo 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 $P \equiv C^d \equiv C^{\overline{e}} \mod p$.

Back to our Example

- Luckily, if $p = 3001$, $e = 7$, then $\gcd(e, p-1) = \gcd(7, 3000) = 1$ so we can decrypt.
- $d \equiv \overline{e} \equiv 2143 \mod 3000$ (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
- Voilà!

What's the advantage?

- "Known-plaintext" attacks
- Consider the additive cipher
- Suppose an attacker obtains a plaintext-ciphertext pair
- E.g. ca $\leftrightarrow$ 0200 corresponds to 1840
- $1840 - 0200 \equiv 1640 \mod 3000$ obtains the key
- The multiplicative cipher works similarly
- Finding the key is approximately the same speed as decryption with key

Pohlig-Hellman resists known-plaintext attacks

- Suppose the attacker obtains $C = P^e$ and P
- Needs to find the "discrete logarithm" $e = \log_P C \mod p$
- Best known algorithm is substantially slower than decryption with key
- Why isn't Pohlig-Hellman used in practice?

Pohlig-Hellman resists known-plaintext attacks

- Suppose the attacker obtains $C = P^e$ and P
- Needs to find the "discrete logarithm" $e = \log_P C \mod p$
- Best known algorithm is substantially slower than decryption with key
- Why isn't Pohlig-Hellman used in practice?
  - It's slower than other private key ciphers which also resist known-plaintext attacks

So why should we care?

- RSA also uses modular exponentiation
  - Composite modulus
  - Find decryption key using Euler's Theorem (extension of Fermat's Little Theorem to composite modulus)
- But RSA also introduces idea of public and private keys
  - Encryption key is public
  - Decryption key is private
  - Factorization of modulus is secret; need it to find decryption key
- Pohlig-Hellman provides a gentle introduction
- Other related topics
  - Fast exponentiation
  - Fast primality testing
- Always good to know another cipher!