Math 312, lecture 16, 8/6/2018

Last time: Affine ciphers in $\{0,1,\ldots,25\} = \{A,B,\ldots,Z\}$:

$E(P) \equiv aP+b \ (26)$

$D(C) \equiv \bar{a}(C-b) \ (26)$

Today:

Block (eg cipher: Group letters into blocks (eg. encoded as k-digit numbers to base 26, or vectors of length k)

Remind ourselves: Key is the secret Alice & Bob know that allows Bob to decrypt the message (above the key is $(\bar{a},-b)$ $\rightsquigarrow$ (a,b))

Today: RSA

Key innovation: "public-key crypto": encryption key used by Alice is public.

(decryption key, used by Bob is secret)

Method: Bob chooses two large primes $(p \neq q)$

(current usage usually $p,q \sim 2^{2048} \sim 10^{600}$)

Bob sets $m = pq$. Bob chooses d,e mod $\phi(m) = (p-1)(q-1)$

s.t. $de \equiv 1 \ (\phi(m))$.

Bob keeps (p,q,d) secret. Bob publishes (m,e)

↑ "secret key" "decryption key".

↑ "public key" "encryption key"

Messages encoded as classes mod m
(actually ~~invertible~~ invertible classes)

Encryption: $E(P) \equiv P^e \pmod m$

Decryption: $D(C) \equiv C^d \pmod m$

HW: $(P^e)^d \equiv P^{ed} \equiv P \pmod m$ since $ed \equiv 1 \pmod{\phi(m)}$
and (Euler's thm) $P^{\phi(m)} \equiv 1 \pmod m$

(If Eve can factor m, she can learn p, q thus $\phi(m)$ thus d)

Example: $p=5$, $q=7$, $m=pq=35$, $\phi(m)=4\cdot 6=24$
can take $\boxed{d=7, e=7}$ or $d=5, e=5$

Encode 17. by repeated squaring

(1) write $7 = 4+2+1 = 2^2+2^1+2^0$ | $5 = 2^2+2^0$

(2) $17^7 = 17^4 \cdot 17^2 \cdot 17^1$ | $17^5 = 17^4 \cdot 7^1$

repeated squaring:

(3) $17^1 \equiv 17 \pmod{35}$
$17^2 \equiv 17\cdot 17 = 289 \equiv 280+9 \equiv 9 \pmod{35}$
$17^4 = 17^{2\cdot 2} = 17^2 \cdot 17^2 \equiv 9\cdot 9 = 81 \equiv 11 \pmod{35}$

(4) $17^7 \equiv 11\cdot 9\cdot 17 \equiv 99\cdot 17 \equiv -6\cdot 17 \equiv$
$\equiv -102 \equiv 3 \pmod{35}$

| $17^5 \equiv 11\cdot 17 = 187$
$= 175+12 \equiv 12 \pmod{35}$

Se If $e=7$, $\epsilon(17) \equiv 3 \pmod{35}$

If $e=5$, $\epsilon(17) \equiv 12 \pmod{35}$

Example: $p^{100} = p^{64+32+4}$, compute $p^1, p^2, p^4 = (p^2)^2, p^8 = (p^4)^2$, $p^{16} = (p^8)^2$, $p^{32} = (p^{16})^2$, $p^{64} = (p^{32})^2$

then mult $p^{100} = p^{64} \cdot p^{32} \cdot p^4$

Need only 8 multiplications, not 99 ($p^{100} = \underbrace{p \cdot p \cdot p \cdots p}_{100}$)

Decryption: $3^7 \equiv 3^4 \cdot 3^2 \cdot 3^1 \equiv (3^2)^2 \cdot 3^2 \cdot 3$

$\equiv 3 \cdot 9 \cdot 81 \equiv 27 \cdot 11 \equiv -88 \equiv -18 \equiv 17 \pmod{35}$

$27 \equiv -8 \pmod{35}$

Aside: RSA is fast enough to work,
too slow for encryptic large amounts of data
Actually used to exchage keys for faster symmetric cipher

Another application: digital signatures

- Encryption was based on $D(E(P)) = P$

But RSA also satisfies $E(D(C)) = C$.

Bob can prove "I am the person who can factor m".

Bob choose a random number C, publishes $(C, D(C))$
i.e. (C, C^d) anyone can check: $(C^d)^e \equiv C \pmod{m}$

Bob can also sign messages: Bob has message P.
Bob can send the pair (P, P^d)
Alice can verify integrity of communications by checking if

$$(P^d)^e \equiv P \pmod{m}$$

These ideas depend on hardness of the discrete logarithm problem: given (C, C^d) hard to compute d.