Lecture 23: Very brief intro to cryptology, to motivate More Number Theory

Dave Naumann

Department of Computer Science
Stevens Institute of Technology

CS 135 Discrete Structures Spring 2015

Alice and Bob

Alice wants to send message m to Bob. We may as well consider m to be a natural number (the binary encoding of the music or whatever Alice is sending).

Alice doesn't want anyone else to get the message, so she needs a secret way of scrambling m, that Bob can invert but no one else can (so he shares the secret).

Not easy to do this without being vulnerable to Eve having smart way to unscramble.

Cryptanalysis: study of ways to break ciphers. ETAOINSHRDLU
To decrypt ciphertext "VGCUG", guess that G stands for E —try shifting the other letters back by 2.

So use a well understood function enc with the right properties, which takes an extra parameter, the secret key that only Alice and Bob know.

Alice and Bob

Alice wants to send message m to Bob. We may as well consider m to be a natural number (the binary encoding of the music or whatever Alice is sending).

Alice doesn't want anyone else to get the message, so she needs a secret way of scrambling m, that Bob can invert but no one else can (so he shares the secret).

Not easy to do this without being vulnerable to Eve having smart way to unscramble.

Cryptanalysis: study of ways to break ciphers. ETAOINSHRDLU
To decrypt ciphertext "VGCUG", guess that G stands for E —try shifting the other letters back by 2.

So use a well understood function enc with the right properties, which takes an extra parameter, the secret key that only Alice and Bob know.

Shared key crypto

Usefulness property: has an inverse, dec, so that (dec key (enc key msg)) = msg.

Security: given the ciphertext (enc key msg) but not key, it is difficult to determine msg without doing brute force search:

```
int key; key:=0;
while true do
  if (dec key msg) looks like sensible English
    return (dec key msg);
  else key++;
```

Simple example: $enc(k, plaintext) = (plaintext + k) \bmod N$ where N is some fixed number (at least the number of possible messages). Then $dec(k, ciphertext) = (ciphertext - k) \bmod N$ is an inverse.

Shared key crypto

Usefulness property: has an inverse, dec, so that (dec key (enc key msg)) = msg.

Security: given the ciphertext (enc key msg) but not key, it is difficult to determine msg without doing brute force search:

```
int key; key:=0;
while true do
  if (dec key msg) looks like sensible English
    return (dec key msg);
  else key++;
```

Simple example: $enc(k, plaintext) = (plaintext + k) \bmod N$ where N is some fixed number (at least the number of possible messages). Then $dec(k, ciphertext) = (ciphertext - k) \bmod N$ is an inverse.

Intermezzo on higher order functions

Suppose the experts have published good enc and dec functions.

If Alice and Bob share a secret number, they can get their own secret functions.

```
(define (encrypt key)
  (lambda (plaintext) (enc key plaintext)))
(define (decrypt key)
  (lambda (ciphertext) (dec key ciphertext)))

(define ourSecretKey 205883846520856388483824002658)
(define ourSecretEnc (encrypt ourSecretKey))
(define ourSecretDec (decrypt ourSecretKey))
```

Beyond shared keys

Everyone knows enc and dec. How do Alice and Bob agree on key in the first place, while keeping it secret from everyone else?

(Alice is in a cybercafe in Tibet and Bob is in Arkansas.)

Idea: find enc and dec that don't use the same key.

Bob broadcasts a public key e but keeps his own secret key d.

Alice sends (enc e msg). Bob computes (dec d stuff-he-receives).

Usefulness property: (dec d (enc e msg)) = msg.

Security: given both e and (enc e msg), it's intractable to find d (or otherwise find msg) without doing brute force search.

Beyond shared keys

Everyone knows enc and dec. How do Alice and Bob agree on key in the first place, while keeping it secret from everyone else?

(Alice is in a cybercafe in Tibet and Bob is in Arkansas.)

Idea: find enc and dec that don't use the same key.

Bob broadcasts a public key e but keeps his own secret key d.

Alice sends (enc e msg). Bob computes (dec d stuff-he-receives).

Usefulness property: (dec d (enc e msg)) = msg.

Security: given both e and (enc e msg), it's intractable to find d (or otherwise find msg) without doing brute force search.

Beyond shared keys

Everyone knows enc and dec. How do Alice and Bob agree on key in the first place, while keeping it secret from everyone else?

(Alice is in a cybercafe in Tibet and Bob is in Arkansas.)

Idea: find enc and dec that don't use the same key.

Bob broadcasts a public key e but keeps his own secret key d.

Alice sends (enc e msg). Bob computes (dec d stuff-he-receives).

Usefulness property: (dec d (enc e msg)) = msg.

Security: given both e and (enc e msg), it's intractable to find d (or otherwise find msg) without doing brute force search.

Beyond shared keys

Everyone knows enc and dec. How do Alice and Bob agree on key in the first place, while keeping it secret from everyone else?

(Alice is in a cybercafe in Tibet and Bob is in Arkansas.)

Idea: find enc and dec that don't use the same key.

Bob broadcasts a public key e but keeps his own secret key d.

Alice sends (enc e msg). Bob computes (dec d stuff-he-receives).

Usefulness property: (dec d (enc e msg)) = msg.

Security: given both e and (enc e msg), it's intractable to find d (or otherwise find msg) without doing brute force search.

Review

If $a \mid b$ and $a \mid c$ then $a \mid (mb + nc)$ for $a, b, c, m, n \in \mathbf{Z}$

For $m \in \mathbf{Z}^+$, $a = (a \mathbin{\mathbf{div}} m) \cdot m + (a \mathbin{\mathbf{mod}} m)$

If $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ (for positive integer m) then $a + c \equiv b + d (\text{mod } m)$ and $ac \equiv bd (\text{mod } m)$

$(a + b) \mathbin{\mathbf{mod}} m = ((a \mathbin{\mathbf{mod}} m) + (b \mathbin{\mathbf{mod}} m)) \mathbin{\mathbf{mod}} m$

$ab \mathbin{\mathbf{mod}} m = ((a \mathbin{\mathbf{mod}} m)(b \mathbin{\mathbf{mod}} m)) \mathbin{\mathbf{mod}} m$

If $gcd(a, b) = 1$ then a, b are called *relatively prime*

Linear combination Thm:
$\forall a, b \in \mathbf{Z}^+.\ \exists s, t \in \mathbf{Z}.\ gcd(a, b) = sa + tb$

From which we proved, in last lecture:
Lemma X: for $a, b, c \in \mathbf{Z}^+$, if $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

In search of invertible operations: division

Recall that multiplication respects congruence:

$a \equiv b (\text{mod } m) \to ac \equiv bc (\text{mod } m)$

Not so division: $14 \equiv 8 (\text{mod } 6)$ but $14/2 \not\equiv 8/2 (\text{mod } 6)$

For c relatively prime to m, division does work:

Thm: If $ac \equiv bc (\text{mod } m)$ and $gcd(c, m) = 1$ then $a \equiv b (\text{mod } m)$.

Proof:

1. $m \mid (ac - bc)$ from assumption $ac \equiv bc (\text{mod } m)$ by def
2. $m \mid (a - b)c$ from 1 by arith
3. $m \mid a - b$ from 2 by assumption $gcd(c, m) = 1$, Lemma X
4. $a \equiv b (\text{mod } m)$ from 3 by def

In search of invertible operations: division

Recall that multiplication respects congruence:
$a \equiv b (\mathrm{mod}\ m) \to ac \equiv bc (\mathrm{mod}\ m)$
Not so division: $14 \equiv 8 (\mathrm{mod}\ 6)$ but $14/2 \not\equiv 8/2 (\mathrm{mod}\ 6)$

For c relatively prime to m, division does work:

Thm: If $ac \equiv bc (\mathrm{mod}\ m)$ and $gcd(c, m) = 1$ then $a \equiv b (\mathrm{mod}\ m)$.
Proof:

1. $m \mid (ac - bc)$ from assumption $ac \equiv bc (\mathrm{mod}\ m)$ by def
2. $m \mid (a - b)c$ from 1 by arith
3. $m \mid a - b$ from 2 by assumption $gcd(c, m) = 1$, Lemma X
4. $a \equiv b (\mathrm{mod}\ m)$ from 3 by def

Linear congruence

How to solve $ax \equiv b(\text{mod } m)$ for x (assume $m > 1$)?
Find an "inverse", $\overline{a}$, s.t. $\overline{a}\,a \equiv 1(\text{mod } m)$, solution is then $\overline{a}\,b$.

Thm: If $gcd(a, m) = 1$ and $m > 1$ then $\exists \overline{a}.\ \overline{a}\,a \equiv 1(\text{mod } m)$

1. $sa + tm = 1$ for some s, t, by $gcd(a, m) = 1$, Lin Comb Thm
2. $sa + tm \equiv 1(\text{mod } m)$ from 1
3. $tm \equiv 0(\text{mod } m)$ by property of "$\equiv$ mod m"
4. $sa \equiv 1(\text{mod } m)$ from 2,3 (by property of "$\equiv$ mod m")
5. $(s \textbf{ mod } m)a \equiv 1(\text{mod } m)$ from 4

So $(s \textbf{ mod } m)$ is the $\overline{a}$ we need.

Are there other conditions under which a might have an inverse?

Linear congruence

How to solve $ax \equiv b \pmod{m}$ for x (assume $m > 1$)?
Find an "inverse", $\overline{a}$, s.t. $\overline{a}\,a \equiv 1 \pmod{m}$, solution is then $\overline{a}\,b$.

Thm: If $gcd(a, m) = 1$ and $m > 1$ then $\exists \overline{a}.\ \overline{a}\,a \equiv 1 \pmod{m}$

1. $sa + tm = 1$ for some s, t, by $gcd(a, m) = 1$, Lin Comb Thm
2. $sa + tm \equiv 1 \pmod{m}$ from 1
3. $tm \equiv 0 \pmod{m}$ by property of "$\equiv \bmod m$"
4. $sa \equiv 1 \pmod{m}$ from 2,3 (by property of "$\equiv \bmod m$")
5. $(s \mathbin{\mathbf{mod}} m)a \equiv 1 \pmod{m}$ from 4

So $(s \mathbin{\mathbf{mod}} m)$ is the $\overline{a}$ we need.

Are there other conditions under which a might have an inverse?

Linear congruence

How to solve $ax \equiv b \pmod{m}$ for x (assume $m > 1$)?
Find an "inverse", $\overline{a}$, s.t. $\overline{a}\,a \equiv 1 \pmod{m}$, solution is then $\overline{a}\,b$.

Thm: If $gcd(a, m) = 1$ and $m > 1$ then $\exists \overline{a}.\ \overline{a}\,a \equiv 1 \pmod{m}$

1. $sa + tm = 1$ for some s, t, by $gcd(a, m) = 1$, Lin Comb Thm
2. $sa + tm \equiv 1 \pmod{m}$ from 1
3. $tm \equiv 0 \pmod{m}$ by property of "$\equiv \bmod m$"
4. $sa \equiv 1 \pmod{m}$ from 2,3 (by property of "$\equiv \bmod m$")
5. $(s \bmod m)a \equiv 1 \pmod{m}$ from 4

So $(s \bmod m)$ is the $\overline{a}$ we need.

Are there other conditions under which a might have an inverse?

Instantiation

In proving the Lemma (last lecture), we concluded $a \mid (sac + tbc)$ from $a \mid sac$ and $a \mid tbc$. How? By instantiating the lemma "$a \mid b \wedge a \mid c \to a \mid (mb + nc)$." Substituted sac for b, tbc for c, 1 for m, and 1 for n.

Scheme exercise:

```
(define (subst x s1 s2)
  ; Assume s1, s2 are s-expressions and x is an atom.
  ; Transform s1 by replacing every occurrence of x by s2
  to-do
)
```

Instantiation

In proving the Lemma (last lecture), we concluded $a \mid (sac + tbc)$ from $a \mid sac$ and $a \mid tbc$. How? By instantiating the lemma "$a \mid b \wedge a \mid c \rightarrow a \mid (mb + nc)$." Substituted sac for b, tbc for c, 1 for m, and 1 for n.

Scheme exercise:

```
(define (subst x s1 s2)
  ; Assume s1, s2 are s-expressions and x is an atom.
  ; Transform s1 by replacing every occurrence of x by s2
  to-do
)
```

Necessity

We showed that $gcd(a, m) = 1$ is a sufficient condition for there to exist an $\overline{a}$ such that $\overline{a}\,a \equiv 1 (\text{mod } m)$.

Now we'll show it's a necessary condition.

Suppose there exists some b such that $ba \equiv 1 (\text{mod } m)$.

1. $m \mid (ba - 1)$ from supposition
2. $ba - 1 = km$ for some k, from 1 by def of $\mid$
3. $ba - km = 1$ from 2 by arith
4. $gcd(a, m) = 1$ from 3 by Lin Comb Thm ????

Actually, that Thm goes the other way and has an existential: if $gcd(a, m) = c$, not every linear comination of a and m is c.

We do get step 4, by this fact: For any b, c, if $ba - cm = 1$ then $gcd(a, m) = 1$. Proof of fact: if $d > 0$ is a common divisor of a, m then $d \mid (ba - cm)$, and $d \mid 1$ implies $d = 1$.

Necessity

We showed that $gcd(a, m) = 1$ is a sufficient condition for there to exist an $\overline{a}$ such that $\overline{a}\,a \equiv 1(\text{mod } m)$.
Now we'll show it's a necessary condition.
Suppose there exists some b such that $ba \equiv 1(\text{mod } m)$.

1. $m \mid (ba - 1)$ from supposition
2. $ba - 1 = km$ for some k, from 1 by def of $\mid$
3. $ba - km = 1$ from 2 by arith
4. $gcd(a, m) = 1$ from 3 by Lin Comb Thm ????

Actually, that Thm goes the other way and has an existential: if $gcd(a, m) = c$, not every linear comination of a and m is c.

We do get step 4, by this fact: For any b, c, if $ba - cm = 1$ then $gcd(a, m) = 1$. Proof of fact: if $d > 0$ is a common divisor of a, m then $d \mid (ba - cm)$, and $d \mid 1$ implies $d = 1$.

Necessity

We showed that $gcd(a, m) = 1$ is a sufficient condition for there to exist an $\overline{a}$ such that $\overline{a}\,a \equiv 1 (\mathrm{mod}\ m)$.

Now we'll show it's a necessary condition.

Suppose there exists some b such that $ba \equiv 1 (\mathrm{mod}\ m)$.

1. $m \mid (ba - 1)$ from supposition
2. $ba - 1 = km$ for some k, from 1 by def of $\mid$
3. $ba - km = 1$ from 2 by arith
4. $gcd(a, m) = 1$ from 3 by Lin Comb Thm ????

Actually, that Thm goes the other way and has an existential: if $gcd(a, m) = c$, not every linear comination of a and m is c.

We do get step 4, by this fact: For any b, c, if $ba - cm = 1$ then $gcd(a, m) = 1$. Proof of fact: if $d > 0$ is a common divisor of a, m then $d \mid (ba - cm)$, and $d \mid 1$ implies $d = 1$.

Necessary and sufficient

Exercise: write a stronger version of the Theorem on Slide 8.