Few remarks on OWFs:

- Work to compute in "forward" direction must be polynomial. ($\leq f(|x|)$ for some polynomial $f$)
- Odds of a bounded adversary succeeding in inversion must be negligible in $|x|$.

  (e.g. $2^{-|x|}$)

---

More OWF candidates: Modular exponentiation / discrete logs.

Say $p=5$, $g=2$. Look at powers of $g$ mod $p$:

$$\boxed{\mathbb{Z}_5 = \{0,1,\dots 4\}}$$

$$g^1 = 2 \pmod 5$$
$$g^2 = 4$$
$$g^3 = 3$$
$$g^4 = 1$$

Observation: taking powers of $g=2$ gave us all values in $1,2,\dots 4$ mod $p=5$

So in this case, the function

$$x \longmapsto g^x \bmod p$$

is a permutation of the integers $1,2,\dots,p-1$.

Looking ahead: we'll see this was no accident: for any prime $p$, we can find $g$ s.t.

$$\{g^1, g^2, \dots g^{p-1}\} = \{1,2,\dots,p-1\}$$

OWF candidate (actually a OW Permutation):

$$x \longmapsto g^x \bmod p \quad (\text{on } \{1,2,\dots p-1\})$$

# Application: Diffie Hellman Key Exchange

Goal: agree on a secret (random) value over a public channel.

$$\text{Alice} \quad \rightleftarrows \quad \text{Bob}$$

s                              s

Eve can't deduce s.

Setup: $p$ prime (say $p \approx 2^{1000}$).

$g \in \mathbb{Z}_p$ s.t. $\{g^1, g^2, \dots g^{p-1}\} = \{1, 2, \dots p-1\}$.
(mod $p$)

| Alice | | Bob |
|---|---|---|
| $a \in_R \{1, \dots p-1\}$ | $\xrightarrow{A}$ | $b \in_R \{1, 2, \dots p-1\}$ |
| $A \triangleq g^a \bmod p$ | $\xleftarrow{B}$ | $B \triangleq g^b$ |
| $s \triangleq B^a$ | | $s \triangleq A^b$ |

$$B^a = (g^b)^a = g^{ba} = g^{ab} = (g^a)^b = A^b \quad \checkmark$$

Note: if DLP is hard, then recovering $a$ from $A = g^a$ is hard for Eve.
Similarly for getting $b$ from $B = g^b$.

This doesn't necessarily preclude computing $g^{ab}$ some other way (w/o knowing $a, b$ directly), but there is no known efficient algo for this setting

(Some caveats about bad choices of $p$ however...)

Recovering $g^{ab}$ from $A, B$ is the "Diffie Hellman problem"

**Loose ends...**

- Efficient computation of $g^a \bmod p$?

  $a, p$ are $\approx 1000$ bits long!!

```
A = 1;
for (i=0; i<a; i++)
{    A*=g;   A %= p; }
```

No! Takes forever! ($\approx 2^{1000}$ steps)

Observation: there are some (very) large exponents of $g$ that we <u>can</u> compute.

E.g. $g^{2^i}$ for "reasonable" values of $i$ (e.g. $i = 1000$).

repeat: $g *= g$ 1000 times!

$$\circledast \qquad g \to g^2 \to g^4 \to g^8 \to g^{16} \to \dots g^{2^i}$$

But this actually gives us what we want! For any exponent $a$, we can get $g^a \bmod p$ by multiplying the right subset of $g^{2^i}$'s:

Write $a$ in binary:

$$a = \sum_{i=0}^{\ell} 2^i \cdot a_i \qquad \text{(where } a_i \in \{0,1\}.)$$

Then compute $\{g^{2^i}\}_{i=0}^{\ell}$.

Then observe that

$$g^a = g^{\sum_{i=0}^{l} 2^i a_i} = \prod_{i=0}^{l} g^{2^i a_i}$$

$$= \prod_{a_i=1} g^{2^i} \quad \checkmark$$

Time? (assume mult / squaring takes $l^2$ steps)

$O(l^3)$

How hard is it to generate parameters? E.g. how hard to find $p$ a large prime? Knowing there are an $\infty$ of primes might not suffice:

$$2, 3, 5, 7, 11, 13, 17 \ldots \quad \underbrace{923459\,97 \quad (2^{100000}-1)}\quad \underbrace{(2^{1000000000}-1)}$$

(gaps could increase in an unreasonable way)

Good news: prime # theorem:

$$\#\text{ primes} < n \approx \frac{n}{\log n}$$

(*) So if we take a random $l$ bit value, odds that it is prime would be $\approx 1/l$

Not too bad ... provided we have an efficient <u>test</u> for primality. And indeed we do!

Easy version: Fermat test. To check if $p$ is prime: choose $a \in 1, \ldots, p-1$

and make sure $a^p \bmod p = a$

Do this $k$ times. If we <u>always</u>

? $\rightarrow$ get $a^p \bmod p = a$, output "prime"

100% $\rightarrow$ if ever $a^p \bmod p \neq a$, output "not prime".

Turns out there are classes of #'s that can fool this test every time (Carmichael #s)

However, there is a similar test that does not have this flaw (Miller-Rabin). Really good error bounds! (Very unlikely to get a false positive.)

And if you're willing to spend $\Theta(\ell^6)$ time, there's a deterministic test (discovered $\approx$ 2000 by A.K.S.)

— How to find $g$ s.t. $\{g^1, g^2, \ldots g^{p-1}\} = \{1, 2, \ldots p-1\}$ ? (mod $p$)

When $p$ is not prime, no such $g$ exists.

Fact: such $g$ always exists when $p$ is prime.

Proof: not now...

Related: when does $x \in \mathbb{Z}_n$ have a multiplicative inverse?

(i.e., $\exists\, y \in \mathbb{Z}_n$ s.t. $xy = 1 \bmod n$)

Turns out $x$ is invertible $\Leftrightarrow$ $\gcd(x,n) = 1$.

<u>Reason</u>: $\gcd(x,n) = ax + bn$ for some $a, b \in \mathbb{Z}$.

(Note: $a, b$ efficiently computable via xgcd algo.)

Say $\gcd(x,n) = 1$. Then $1 = ax + bn$ for some $a, b \in \mathbb{Z}$. $\therefore$ $a = x^{-1}$!

$$1 - bn = ax$$

Now reduce mod $n$: $\quad 1 = ax \mod n.$

$$x = y \Rightarrow x \% n = y \% n$$

Want $ax \equiv 1 \mod n.$

Could just reduce $a$ mod $n$ if necessary to set the "least residue". Say $a > n$. Then define $a' = a \% n$.

$$a = \underbrace{k}_{= a/n} n + \underbrace{a'}_{= a\%n}, \quad a' < n.$$

$$ax = (kn + a')x \equiv 1 \mod n$$

$$(= 1 + jn \quad \text{Some } j \in \mathbb{Z})$$

$$\therefore \quad knx + a'x = 1 + jn$$

$$\Rightarrow \quad a'x = 1 + jn - knx$$

$$= 1 + \underbrace{(j - kx)\,n}_{= 0 \mod n}$$

Perfect. $a' = x^{-1}$

Converse? $\gcd(x,n) > 1 \Rightarrow$ no inverse for $x$.

Turns out that anything of the form

$$\{ax + bn \mid a, b \in \mathbb{Z}\} \quad \text{is}$$

a multiple of $d = \gcd(x,n)$.

So if $\exists\ a \in \mathbb{Z}$ s.t. $ax \equiv 1 \mod n$

Then $ax = 1 + bn$.

But then $ax - bn = 1$ ※

(1 not a multiple of $d > 1$)

So indeed, $x^{-1}$ exists $\iff$ $\gcd(x,n) = 1$. ✓

<u>Notation</u>: define $\mathbb{Z}_n^* \triangleq \{x \in \mathbb{Z}_n \mid \gcd(x,n) = 1\}$.

<u>Examples</u>: $\mathbb{Z}_6^* = \{1, 5\}$

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ if $p$ is prime.

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

Question: what is $|\mathbb{Z}_n^*|$? (How many elements?)

Easier question: what is $|\mathbb{Z}_{p^k}^*|$? ($p$ prime)

Hint: write elements of $\mathbb{Z}_{p^k}$ in <u>base $p$</u>:

$$x = \square \cdot p^0 + \square \cdot p^1 + \square \cdot p^2 + \cdots + \square \cdot p^{k-1}$$

($\square$'s $\in 0, \ldots p-1$)

How many ways to fill in $\square$'s w/ values in $0, \ldots p-1$ so as to not get a multiple of $p$?

$$x = \boxed{p-1 \text{ choices}} \cdot p^0 + \boxed{p \text{ choices}} \cdot p^1 + \cdots + \boxed{p \text{ choices}} \cdot p^{k-1}$$

$\therefore |\mathbb{Z}_{p^k}^*| = p^{k-1} \cdot (p-1)$

<u>Fact</u>: if $\gcd(n,m)=1$,

Then $|\mathbb{Z}^*_{nm}| = |\mathbb{Z}^*_n|\cdot|\mathbb{Z}^*_m|$

This, combined w/ the above gives a formula for any integer (provided you know the factorization!)

<u>Notation</u>: $\varphi(n) \triangleq |\mathbb{Z}^*_n|$.

"Euler function"

(above, rephrased: $\gcd(n,m)=1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$)

<u>Notation</u>: $\langle g \rangle = \{g^1, g^2, g^3, \ldots\}$

How to find $g \in \mathbb{Z}^*_p$ s.t. $\langle g \rangle = \mathbb{Z}^*_p$?

Method: guess and check... :-(

Not so bad if factorization of $p-1$ is known.

Good news: "easy" to choose $p$ so that you know how $p-1$ factors into primes.

(We'll come back to this...)

---

Candidate OWF: RSA

Setup: let $p, q$ be random $\ell$-bit primes.

Set $n = pq$.

Choose $e \in \mathbb{Z}$ s.t. $\gcd(e, \varphi(n)) = 1$

$\varphi(n) = (p-1)(q-1)$

Public parameters: $n, e$.

Secret params.: $p, q$.

RSA function: for $x \in \mathbb{Z}_n$, $x \mapsto x^e \bmod n$.

Cool feature: <u>invertible</u> if you know $p, q$ !!