The Discrete Logarithm Problem

Let $p$ be a prime, and $g \in \mathbb{Z}_p^*$ of large order.

In particular $g$ is \textit{primitive} if $\text{ord}_p g = p - 1$.

The function $x \mapsto g^x \mod p$
seems to be one-way. In other words,

\textit{given $b$, $g \in \mathbb{Z}_p^*$, it is difficult to find an integer $x$ such that $b \equiv g^x \pmod{p}$}. 

© 2011 Clifford Bergman
\[ b \equiv g^x \pmod{p} \]

Note that, given \( b \), \( x \) is unique modulo \( \operatorname{ord}_p g \).
Write \( x = \log_g b \),

the \textit{discrete log} of \( b \) to the base \( g \).
The El Gamal Cryptosystem

Choose a prime $p$, an element $g \in \mathbb{Z}_p^*$ of large order, and an integer $a$. Let $b = g^a \% p$.

**Public Key:** $(p, g, b)$

**Private Key:** $(p, a)$.

**Encryption:** Choose a (secret) random integer $k$.

$E(m) = (g^k \% p, mb^k \% p)$. \hspace{1cm} (m \in \mathbb{Z}_p^*)

**Decryption:** $D(y, z) = z(y^a)^{-1} \% p$. 

© 2011 Clifford Bergman
Does it work? I.e., does $D(E(m)) = m$?

$E(m) = (g^k \% p, mb^k \% p)$

$D(g^k, mb^k) \equiv_p mb^k \cdot (g^{ak})^{-1} \equiv_p m \cdot g^{ak} \cdot g^{-ak} \equiv_p m$. 
Notes

- \( E(m) = (g^k \mod p, mb^k \mod p) \)
  Thus \( E(m) \) is twice as long as \( m \).

- Because of \( k \), every message has multiple encryptions.

- We may as well choose \( a \leq \text{ord}_p g \)
  Thus \( \text{ord}_p g \) should be very large to preclude exhaustive search.

- \( \text{ord}_p g \) is a divisor of \( p - 1 \) (Lagrange).

- Unlike in RSA, \( p \) and \( g \) can be shared by everybody.

\( c \odot 2011 \) Clifford Bergman
Two schools of thought on the choice of $g$

- $g$ a primitive element mod $p$ (i.e. make $\text{ord}_g$ as large as possible)
- Choose $g$ with $\text{ord}_p(g) = q$ a large prime [necessarily, $q \mid (p - 1)$]
Security of ElGamal

Obviously, if the discrete log problem for $p$ can be solved, then ElGamal would be compromised.

Converse is open.

Note that it is important for the sender to keep $k$ secret.
ElGamal Signatures

$p$ a prime, $g \in \mathbb{Z}_p^*$ of large order $n$, $a < n$ $b = g^a \mod p$.

Public Key: $(p, g, b)$
Private Key: $(p, a)$

For message $m < n$

**Signature:** pick a random $k < n$. Let

$$y = g^k \mod p$$

$$S(m) = (y, (m - ay)k^{-1} \mod n)$$

**Verification:** $V(y, z) : b^y y^z \mod p = g^m \mod p$. 
As before, \( p \) and \( g \) can be shared

In practice: given a (long) message \( M \), hash function \( H \). let \( m = H(M) \). Sign \( m \).
Send \( M \) together with \( S(m) \) [and \( H \)].

Every message has multiple valid signatures
Forging a signature

Wish to forge Bob’s signature on message $m$. Need to construct $(y, z)$ such that

$$b^y y^z \equiv g^m \pmod{p}$$

Pick $y$, solve for $z$:  
$$z = \log_y (g^m b^{-y})$$

Pick $z$, solve for $y$:  
$$b^y y^z \equiv g^m$$
Security problems

- If $S(m) = (y, z)$ is a valid signature, and the value of $k$ becomes known, then $a$ is compromised.

\[
z \equiv (m - ay)k^{-1} \pmod{n} \implies a = (m - zk)y^{-1} \mod{n}.
\]

But what if $y$ is not invertible modulo $n$?
If messages $m_1 \neq m_2$ are signed using the same $k$, then $k$ is compromised.