The Elgamal Cryptosystem

- Named after Taher Elgamal who published a description of the cryptosystem in 1984. He was a student of Martin Hellman.

Let $p$ be a prime number. An element $g \in \mathbb{Z}_p$ is a generator or a primitive root modulo $p$ if for each positive integer $i$ in $\mathbb{Z}_p$, there is an integer $k$ so that $g^k \mod p = i$.

Example.

- There are $\phi(\phi(p)) = \phi(p - 1)$ generators in $\mathbb{Z}_p$.
- The following can be used to test if $g \in \mathbb{Z}_p$ is a generator:

  **Fact:** For each prime factor $p_i$ of $p - 1$, $g^{(p - 1)/p_i} \mod p \neq 1$ if and only if $g$ is a generator of $\mathbb{Z}_p$.

  Example cont’d.
Making use of the above fact though is tricky because it would require that we know the factors of \( p - 1 \) – which we know is not easy in general. Hence, in using the Elgamal Cryptosystem we will make this assumption: \( p \) is chosen so that finding a generator \( g \) of \( \mathbb{Z}_p \) is not hard.

The security of the Elgamal Cryptosystem rests on the \textit{discrete log problem}:

\textit{The Cryptosystem:}

Key generation:

Encryption step:
Decryption step:

*Elgamal in practice:*

1. It is important that the modulos \( p \) be large.

2. It is important that when Alice sends her messages, she uses a new random number each time.

3. In general, Elgamal can be used wherever RSA is used.
Key Exchange

A key exchange protocol is a cryptographic approach to establishing a shared key through an insecure channel. We shall assume that an adversary can only eavesdrop, not modify messages that go through the channel.

The Diffie-Hellman (DH) Protocol

Security of the DH protocol

Why the DH protocol cannot withstand a man-in-the-middle attack
Extensions of the DH protocol