

# Key Signing Party

Join the NMT ACM for a GPG key signing party. Prove your identity to other GPG users and build your web of trust!

## What's GPG?

GPG, the Gnu Privacy Guard, is an asymmetric encryption system that allows you to send and receive files and emails under encryption – so that no one else can read them. It also allows you to sign files and messages, proving that you authored them.

## What's a key signing party?

GPG relies on the “Web of Trust” to prove the identity of users. Essentially, if Alice trusts Bob and Bob trusts Charlie, then Alice can probably trust Charlie (trust is transitive). In order for this system to work, there needs to be proof of who explicitly trusts who. This is achieved by each user signing the keys of other users who they know they trust.

## How do I participate?

You'll need to set up GPG and create a keypair, if you don't have one already. You'll then need to register and submit your keypair information (key id and fingerprint) to the NMT ACM online. Then, bring identification and your key details to the party on the 24<sup>th</sup>. Visit [acm.cs.nmt.edu/party](http://acm.cs.nmt.edu/party) to register and get full instructions!

**March 1st, 1:00pm, Cramer 213 at NMT.**  
**Register in advance at [acm.cs.nmt.edu/party](http://acm.cs.nmt.edu/party)**



Direct questions to [acm@cs.nmt.edu](mailto:acm@cs.nmt.edu)