





STEAL THIS FLYER! STEAL THIS FLYER! STEAL THIS FLYER!

COMMUNITY JAMBOREE

IMAGINING WHAT THE INTERNET WILL LOOK LIKE IN 5 YEARS

WHO: YOU! ALL ARE WELCOME!

WHEN: WED. OCT. 28TH 6-9PM

WHERE: PARTS AND CRAFTS

577 SOMERVILLE AVENUE

WHAT: * NETWORKING * CRYPTOGRAPHY

BROADBAND INFRASTRUCTURE







BEGIN PGP PUBLIC KEY BLOCK	
gciINxMhXZ4nPt7kXLBrwDYue6U/WYSGGONxzBnz0O91DhBqx	:M84hdfhmn
Ajgz0W5iYHhecI6OoJRc69MS9gHcztIsTv5KVJItgFphQFXnK	(&sd9g6/sv
wzsw32 f/ ' '_ \ / _ \n98sau98u98	
xxccdsd (_ _) (_) a86K2Mzwj+	
vdkm0d8h\ _ / \/jd99s0a9109	
sRaC1JJKJadsakkj0c / _ -09jdalkj1kadIGsyORCWDO	
7VyjDD99AgZIuKpVllCDjtOMKJAuA9bgZODci2vmaVRzAVEoX	
r8Xe0sRaCqRtaQNTGFH86RJo0dyKqBt7FvwktWGC127dkPC2x	_
n18LOmsklnsdv3m91ncmtn4I '_ \ / _` '	
seDshJkLKjkal+1dsVcfgDsS _) (_ _ _	
vbdfM09A8Ka87HJkadnM+dVf / _ _ \ \	
23kscmMN1Jan2HgdfG81445n _ OKla/sHaj243676HaK1 _	
W/Nvk160MVSedqdgVxxm3NjMV0cXyCa1DR3BwEwSoxV2oOYk0	_
OY5252ShsI7+nLDxV6sIuhOqZSLgjijS/ykpVLowKN2hgNHzI	
5Vdhcc8qG0GsHm1F0FTUTKaS7Cr+D9grvyhIGsyORCWDOR1+P	
PEeXMrdseDvAktZl5RynvoVceinFQ2bTYmQXERZ6PG0xifM0k	
ykLcceFaaCLtCfoCY7yNDJeufkaegvdJ1IE51ZWxpY2F0dHUg	
aGF0LmNvbT6Iemfj2ls3ej8nvlauwl3bAwYLCQgHAwIGFQgCC	
wANaP7NetqTbZQuocamiwvuHy6l1miar8h+Ta7AFWR1uAecHq	_
EGf7Vn2fK1q76sq9no0STPF8i3aP3guQMNBFBjyUwQDADm8Mh	
Y19Rhv6Ok6PZ8GEyWCrtRsxxh/VZtmxC3AFN+nF223z7iUjj0	
3DpsZpTmr4sXurX0v17mCFDn7TrH1uxxuuVVnAtARTs4dMs5a	txzeOusyy
END PGP PUBLIC KEY BLOCK	



Common terms used when discussing encryption and information security

Threat Model - A system for determining the level of security that something or someone would need given the assumed abilities of a theoretical attacker.

Plaintext - Content that has not been encrypted.

Ciphertext - Content that has been encrypted.

"**Strong**" **Cryptography** - Cryptography which is designed to be advanced enough that encrypted content cannot be broken without a computer the size of a few galaxies.

Hash - A mathematical proof that verifies content has not been tampered with. Used like a lid seal on a pickle jar.

Off The Record (OTR) - A set of rules for online chat programs to use in order to send and receive encrypted messages between each other. Commonly used to refer to specific chat programs that use OTR.

Fingerprint - A short, unique ID mathematically tied to a larger encryption key, usually a public key. Typically used to help verify you are using the correct public key for a person.

Pretty Good Privacy (PGP) - One of the first strong cryptography software suites made available to non-military in the 90s, now owned by Symantec.

OpenPGP - A set of rules for software to use when encrypting and delivering content between computers. Both PGP and GPG use these rules and can encrypt and decrypt under the same rules.

GNU Privacy Guard (GPG) - Software that implements OpenPGP's rules, usually used for encrypting email.

Public Key - A code used as an ID for you used when someone needs to secure content only you can see. It's like a lock which can be used to secure content only your private key can unlock.

Private Key - A secret code that can encrypt and decrypt content and must never be shared.

Secure Socket Layer (SSL) - A way to secure the connection between your computer and (typically) a website you are connecting to. It encrypts the connection to the site, but the content can still be decrypted by the site.

