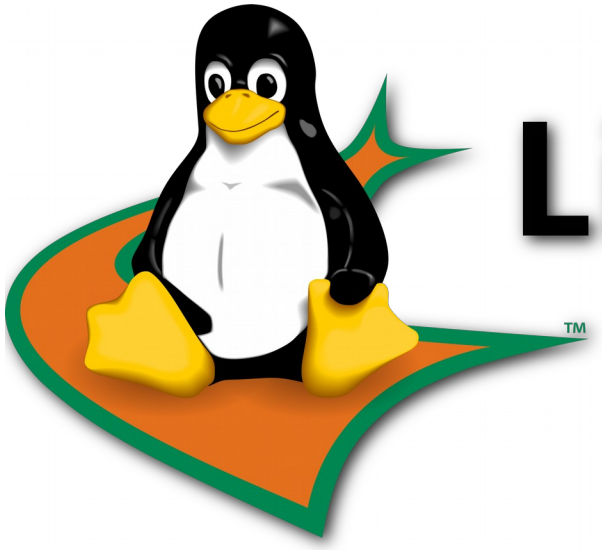
CryptoParty!



Linux Users Group @ UT DALLAS

CryptoParty!

Hang out with us in IRC!

http://lug.utdallas.edu/chat

or

irc.oftc.net #utdlug

What is Encryption?

Unencrypted vs Encrypted

```
<p>Come find out how you can get set up in the cloud quickly and easily so that you h
ave more time to build your project and have fun!</p>

<p>Members of LUG will host a one hour discussion on Git + GitHub and spinning up clo
ud infrastructure on AWS, Google, etc.</p>

<p>Other possible topics include DevOps tools like Vagrant and Ansible, or setting up
 quick solutions on embedded systems.</p>

  <hr />

  <h1>Amazon Web Services Meeting</h1>
  <h3 id="tuesday-march-25-2014--700-pm-in-ti-auditorium-ecss">Tuesday March 25, 2014
 / 7:00 pm in TI Auditorium (ECSS)</h3>

<p><img src="/images/aws.png" alt="Amazon Web Services" /></p>

<p>Interested in Cloud Computing? Want to learn how to deploy your own virtual server
, or host your data in the cloud?</p>

<p>The Linux Users Group @ UTD coordinated with local Amazon reps to host a technical
 introduction to AWS, demonstrating its many services and abilities.</p>

<h4 id="update">Update:</h4>

<p>Here is <a href="https://www.youtube.com/watch?v=KEus17RV1T8">the video stream fro
m this event</a>.</p>

<p>Additionally, the slides are <a href="https://github.com/utdlug/lug-site/blob/mast
er/public/res/aws.pptx?raw=true">available for download</a>.</p>

  <hr />



      </section>
    </div>
    <!--[if !IE]><script>fixScale(document);</script><!--<![endif]-->
  </body>
</html>

16:30:06.627428 IP 129.110.92.80.80 > 10.21.37.24.50268: Flags [F.], seq 9526, ack 82
, win 227, options [nop,nop,TS val 303183305 ecr 3447533], length 0
E..40.@.=....n\P
.%..P.\...d.    N*..........
..5..4..
```

```
..AR./.J.%.E..f........wp..JaC....B..Ou>5...s..1l..d..z.Yo....#./A.....X.........+(.
.......(.K.?|8.."..wu...<$......iJ.x..r2..n~.;.........g.8.fOw......(..S>...V....6..
....6..E'...e....X.>.r.N{U&../...#P....V..gMu.. /...+..dg.c      ..b........r.Z....4O
.u.46...c.....7.....#e.TU.....a'\...).... ..d..\&.>w6C.7..&URXk.,.'zRB.._>      .o.S
....&...=.p...@.G.....y.#%x...;(..g.....8....S..7.q..G*hi....6.M         .....Y.?6`..
.....K.j.....8..&...;"v.,e8.vPy.(]....z1....jX......n.R.y..+E.........  .f
./4.$..S.>}.0i..r2...w.$~^..,x..g..:.    .`.P..~'..g_hNRy..:v..I...,W(.d....$.N`.Y4.c
AH..........).(....g.."./.Z.o..h.Yq...|c.....&N..rf....U...7L.A.-.y.R.../s..A..<#YA
.........{.?.....5....(...A....u.U#..Q.a...of...Y..T.T._..}PW]..r..........&A.u.N~..
.2..jaah>.}/P.SIe0x....^..|....Z@...`C....N......9CQu.y..(...GHO.\A...b,........;.{.
..M..J .....r......'....P.<~.Y@.j..|......h....x..7^.-..N.j..!T..D...@..^:Zb...>X...
.#Ey..YM......g...uG..I..X.....Wn8\...BZ{~f{.......h.3.'*e....`....n.+x.R......hO/..
I.T$...\~[nf..U^.|..T."$Ct.....T/.....D*....t:..3nc_...mi..z.C.r....S.y......d=.vx.%
I.3....J..      uk...MAd....p-.........".L.c.B.......k`.R..!.Zkx;..<h...s..w.g{.....m
....q.c..2.SkY......h..Q.6..Y.c.R
P...m.....KjH.....".D..$...*...b..L................YG....w..o{.......E.hvf......g...
/S^..O.O..0j|...k..l....4......=...0......@.d...k.(=..%TU.g."......|0D...."...v...BC
......:......F;w... c)......,.#.K.1e..;........C..].\6+?..H.3GX.[>.`..n...$.b.......
..?5..x.....F..{,.1..jz......9.h\..........I.........7.......H@...../^|uP....R..3...
...S.a......<.N1p..
L3u\.65(..,F.....8.X2[..Hr..*.y........'....z...KL.3...W.y....VNB.x..w......$.$G...[
/D.....t..u.&...`....0` .........9.E7.qR...|..Jb.f.L.h.....5    .9.ha.\.o..'..n.`9.,
.=......
.n...,.5..uk8..,lY..>.............v.c.n%&D...:O.........n.....|%"......._.4..H......
...+......C..%X.U?g..S..S.5=.sdB.oO...!.1...F.....      6.28.....eJ...|\.Wk....l.8.P
..Q.....tx.....[.D...(M.Yi5....9`G...:Y.=PH.8...Dp*.nt.KO.u..D51%....5...C.!.."   ,
.b].^=uC:.Ed...T.S..4.B@vE......f.G......q}.~H.c..@!.0...RB..X.Y..v:.N...../.Y9.j./g
L.im........1.E.\P;..~.8.no..WY.%.8.gp...kf........S.[...\-Ws..}...=(.m-B.........o?
.t9s.....qM%.E.o-.h......`...P.aT......lBw...n.O.....I..g.......#.....1.;..dH..-..h.
...#......;3O@..h...Q.5u...t.3.S.k.TAVV.]..c...;D5\..6......,X...r$...i..d.......(p.
.......7.48.Q..:..>..|.'G...C...\...uq..^.R..(.R.D...}.........{.<..l{..x..VD&..?...
....C...C.
x...AaX].uM...#).......6(:./.+wY-..x.'X0P...b.......s..BW...,.YOBx.sf..{+y.
..;..*.F..H.|ge...O.]..#..)}.&L]...{..T...w..j.m.jaK...K.p>< ....v*.i.u%.>.......h_x
7P.)$..`....{........l......7.P.h....%.2~..$.....yCN...._aO...)J..6...#4..ZeV.(.`+..
..      ..n.-....`.~b.8./..W.\.}"P...bU....i.V~.....0.Ag.......1n....S..f8}.hT.+.?t.
.[%akS.BI..I..B...7.^.....G.=....y.6.rZT...
16:30:09.430040 IP 129.110.92.80.443 > 10.21.37.24.46180: Flags [F.], seq 16052, ack
 784, win 235, options [nop,nop,TS val 303184006 ecr 3450336], length 0
E..4..@.=.JK.n\P
.%....d....Z-.y..........
..8..4..
16:30:09.431916 IP 129.110.92.80.443 > 10.21.37.24.46180: Flags [.], ack 785, win 23
5, options [nop,nop,TS val 303184006 ecr 3450338], length 0
E..4..@.=.JJ.n\P
.%....d....Z-.z..........
..8..4..
^[
```

Dark Math Magic

$$m^{ed} = m^{1+h\varphi(n)} = m\left(m^{\varphi(n)}\right)^h \equiv m(1)^h \equiv m \pmod{n}$$

What is Encryption?

- **Prime numbers are easy to generate**
  - But it is hard to find a prime factorization
- **Modulus is one-way math**

Private key decrypts and signs

Public key encrypts and verifies

OpenPGP

The world needs a message encryption standard

- Sign Emails
- Encrypt Files
- Share public keys
- Manage private keys

GnuPG

Linux needs an implementation

GnuPG

Installing is easy

```
sudo apt-get install gnupg2 gnupg-agent
sudo apt-get install pinentry-gtk2
```

GnuPG

- Generate a private/public key pair
- Encrypt a file
- Decrypt the file
- Export your public key
- Encrypt an email

Other cool stuff

- Encrypt text messages with SMSSecure
- Encrypt chat messages with Signal
- Encrypt a folder with EncFS
- Encrypt your website with letsencrypt
- Encrypt your online presence with HTTPS Everywhere


ENCRYPT ALL THE THINGS!!!