HTTPS Explained

DR KAMI VANIEA
http versus https
https://ally.com

versus

http://ally.com
Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed**
   - No one can read what you sent
   - No one can change what you sent

2. Knowing **who** you are communicating with
   - You are talking to who you think you are talking to and not someone else
Alice wants to talk securely with Bob
She can encrypt the connection (1)
But how can Alice know she is talking to Bob and not talking to Eve? (2)
Man in the middle attack

Alice → Eve → Bob

Eve is the attacker in the middle.
Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed**
   - No one can read what you sent
   - No one can change what you sent

2. **Knowing who** you are communicating with
   - You are talking to who you think you are talking to and not someone else
First, a short primer on encryption.

You will need to understand this eventually, but for now you mostly need to get the general idea of it.
Encryption often depends on keys like the one on the right. These keys are used with a whole pile of math to encrypt and decrypt a file.

Overly simple example:

<table>
<thead>
<tr>
<th>Message</th>
<th>C</th>
<th>R</th>
<th>Y</th>
<th>P</th>
<th>T</th>
<th>O</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>A</td>
<td>Y</td>
<td>S</td>
<td>Y</td>
<td>I</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Encrypted</td>
<td>C</td>
<td>P</td>
<td>Q</td>
<td>T</td>
<td>O</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

My public key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2
mQENBFHMcgABACAC9BYTEODQ6L2LYh4eiN6uASLqgMqFL+SUHrULUVEtnOxAuxXK XoUhrp/9yXoGi833ztxzCQxog3MeSe6o20N6FQxfvaC84bS4jwolle8Wn5SL 8BznqgCpCgXcN2GjFE1HhUaf72C0SoCehPnMehUHiZHkgeg81d45mlrlP41O1t 1apanMsQ0jgHbZ2xwBRBFYydOUTeBtEkOFLyCyD9KohMa1eBh94knwQIxd4zYR QYKX25+M8obCqv++r9C9He9Q57G58W5hF9RO4U52y0Gtw7yQy8Fk4sVp8rK8y7s2xJ3ByH 0Vt7+7L7iS6B9Cu02BD5sV7jIGwYXyVwV9Ud4BAAEOGLebTHwGymFUsuWbGdx dmOusaVwHg0Su25Z5S5Hy3y1A67B8ewC3AKd4YkYqucEqYCOFGQZCBHAFdswB wbnv/RCP5CAxQG6Cg5FgD4JolA6Q58CMRCt8eV9/RZ+5CAxh8cuGwHhK5Gg6C0I5l O3ZbG5w9C4pJaQw3Q5H9ymNzQeF316kC0jDj2/M5+5EGr07P5qfsG5L3o5Fk9xVjXx 8G576oLl8F3k3wvRy63tF7b3JSP3K9Sj701ejvT7Kl8iBN80QDoP6T0GBh+V6kptkk7Y7xyaJ Fp3LcXV0+113+32Z5QYerlCgR9bmyfHMrB7JvU2YCdL7z7oSeF7H3zAgtmg5QzOM Qt4Y7ig2trvmFwv2QaHe9Kv4w8vYwurU18B9hw5hYX30c1sC1YQFQ911p2wwe0Zw27 6dtpynvBpW+1yx1PwW+2f6hmmYM9XZ7aAY2Jh7JY2wzbN80W0ztH0pX9qGQDaT3SSjU wVcJwL1UCyYBtAcIcQgH9bHwBhUkAIgkCWQvWAGhM4AheBAEBQXWMCmM AeBAAoEkEJNZ 5xG9639BjIaJAWHrYfmrXyM6bCEbW5qX1DX0ACdtb17+70WQ0XHs9K4UJcEdc aK 8Y05124zAaT7hfaXZq13p6mEz0G9VYfM5EOskH0wWbgh2OQICnbaIBCJ7Y5M Bibaww0Kw0biV8e4kk4MakKx9NC6Fbw6A6HRL21sVw20D5kVnMkXocbt7bL7nM cC14Cn3oBdr1d126Lyok80h8c66pVwpPl0ajy/EFySU1wq8yp2v624urB4php15Xv X9ebvULU7+PpzaJLIDMDf7yJj5RIF3POZ34dz4cbbkPnM7vuSoy9w2j2h pzv3be3e7Vhw2izw8Yz2XZt11345QWM0JAHwEwCCAYAf1nSpcAgCkQxMw p9p9Hzt28BA+/optc23J2b8y80t417Pp2z1wevDfSaD7m7ye/X6y6lppr7tw XmpflwIrwe6tN5eWNQCOJ1qSy7qy1jVwpjXu7+q0ujkx8HE7CQDG9XTRk6ny 2nucdI30J3C8BBjCwceswL8x19Fp2v62tjU8kbMD0ps82b47trHmXyAylK 41QB1HFLy5gnoz26OhhOhfH50zem1eMei0Et8B638N6w58k83K7jS6/tV2 cLE8bb9Mr8B9eYYp4aQyxj9o6S902H89B46A3a7FtpnWBLBzE9cYK5DcypQ5Gd h7d1zlXk84+1H02s5fjOCIN76nw7yV6m6E8cza5R6P2wPTVhbMyr0BwVS0u6 neFNvUmXehZ79ptB0T186eGbChBTSK/B8dvjrhRFBt3wFyFDweF3ydW94 8pznPisNorri1g062i1Tg8PbBjB/3wJXwM6y5x126r1mnsnuQiyb5u3Fb2Pw2enDuJc 9ac/N3/3WchilFwBd5As0ap1s2+1melFp0lFne2tpztb2j8tpa9q6xO5h1moSDlnH9aV 7f8pfsul8ubgJl2535x326R6Hq5b6lapqa8pt4uhUwvV2Y8QDh10kaFk6gbYQO8cTa P7/Aj0j6Qh4n69w6p6qFK-9kXu5sUE8fBRBprpD2f6QyM9rMYmulsuA9Q0XqEy AEASYLxyG52zaT6dgcRrHmJ0q5OSwU7d/8PS5BYK8N4u3xL3vwFFcFSqjP 43Z/72w/4WVBA18lu3A6YsCV478TXU3XAK3tI686 shifts3wV6byV38dQ6PdN/0eZn/HbUPh5UwL8L8inho3muA/qo/0kdonmswNMn4AH+r 2Qwe6RosyYFg3rv9zuUw8PtryjDIELAlkfb/PN75C5lwRdNNWhDNP6LcPih5M5eHB QBJ3166Sc2PnQ5sw5S3zav2F59pQzDvJ9s1tAM6Lu3oIujwNfP0dODFzB2 T2Qh/DvHrW0rMg52D0K5j8eLbGmg3lAQEAQAAAYBGQ9QOQAQ1WkLJc50yx4JD4AIvA dBAACRC_LDtxZ9/f5Z9h+l8B8q8m9GgHx83P1iKe7Zw8m6Fp9Eg/MQZGZ2 XH463sAVP5y7CytRfjw9vA4100doWt5j/da7WrFZTcndbTqPm/0u5h6N3ZDUsM mCEV9PAy093/4fiB/66gMO3o2O5BU875VzFq4aFz2m830h2bRv7x2kRw9D TDqFQjGZI6eAAdST231Fa0bzyFe5eAV5kRoq20b8bnaNq35S0WD6351yovd LL08b3S70gg7h9Uk8F2zVzXcIumWspL5Rgp35Lc86HsPb8wWvHeMnI4OaJaB YXG3q9gYca3JgqogVLAZqNwSphWvIvE828yf/fEd n=SFK
-----END PGP PUBLIC KEY BLOCK-----
Public/private key cryptography

- Generate two "keys" that are paired
- Whatever one key locks only the other key can unlock
- Public keys are given out to everybody
- Private keys are kept private

My public key

----BEGIN PGP PUBLIC KEY BLOCK----
Version: GnuPG v2

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6wuLqZmpfL45+SohU4EVLnzsxAUXXH
KoFhef9/Y90g9J8/9332tszxG3gB3M5eSeed06INfoaVaCB948wpo7THhW5y
2BdznpC1pgxCH2G1azAeHUIa7F270COZObC8rPmeslUzHeZ+k+z6datXm118p4010t
1egsdM0Qg09hu22w3R8YIYdU0suetekCrFuRCy7F6KmdMa1eBHH49nrWIt2dIUQ
Y2KX5+M8dC8+R+c9H6an7EG5WHOFWR4DUSY2OrOfvpQzkkR7zu3z39HyHi0
B/h7yi7M6Qb0U22BD5w7iQ7gyKYVsUj0DABEAAGAAIHbhwGvMfuHw0x
dmfuaVnhGzlsZ2sS5YJ5s1aJAI8EEw4EACKFAY9eCfYMCQAZmuAYVcKw
XbW40ACWvYqC5ACsGf8gDAGOfekA4GCACDkxwh911Ph7+C1ACF8o4BqJwGS
GW8Hdkg4y8nDxwq37P3HymyZmQen71a13cKr0j12bQ75/7JzEGh09H0P01fg
8y5x6p3AfE8K3f33G2dWFP0H/dnQyMM8G7f1EG30o32eeQrZqksod3B1p
Sv5CRRydK1+T9H5c05fL772P8oYrQ1X78aIN8KQOpF60dBhRm+Uw7py7e
Ja5nq0PoX1+113T2QY9zctVeYgbwVMhMrP1B2VYCD0zju7qSeFhZmHmgOMmQZd4
Y'15r5w5FmWfaw2ozlheEdv9/4BvnwMyN89jYHGW5HSc0GcPCBZq2k00owlw26T
ipdrwCgWP1LYp1Wf2hbnm1YKza27Jl2bjZvW7ZTWZv7PHok9gkZq87TAjLAb
lwMLCvYyAc1CyGc0WhbIIBHuAkqGwcCNQwMA4Ah4AmibAE0QbWCmMeneMhAK0AE0J2
zQX3B9bAkJw1AgWYrmfYykM6FelSWMhvJ14dX0K1cb17FOV0Q2hsk1qQ0EcLr
+BYa0WfXyHx30zF6eeC02hQYMG2Gkw0vWnhh5eZCwHxqHvRlLQJ0ZmWm
Bilawow0Kw0ib9e4akMakCxcFSBFxe6aHRl0s1v520DikvMnKc0kkcbu70bkLM
cc/Jul0dtk1Bk0nu50l0Kz0nS/vy30jDj0/05Y/eUvO9oy6g2ywv/PQe9eh1Xslye1G
9wB0uUzu3/Pr4pljLMDSSeftY/73X569g3P0ZDNdC40xevKoPnWThYn0yoA0
pzbv3ge7VHwVzIw8wY2zX7T1345WRMOJ1AhJeWECAVAFHYnSpEmcAgcKv9m
p9H9t28BA/o+CuOncN2bUB2BOyt4I77PZe2we/Defa581vmf7YXV/E6yYyPfFr3w
XmF6RlUweye7/NeBwWlCCz06YyVxjL3wJTu/Q3hKhj5s8E7GQXCTR5Eny
2n0dci0/2ZC382JCuwwx6oF1x79P1+2Vg6uUkmD0ps2b8bhtwHmXMLy
41QDHbLYSjzlzw02/3h0dHcf0H9Z0emn5Me6lEeK6888B3swvB5bK8t+skZ/L
-OEP9BBM9B8mYg6aPwRyYckmX1LM889aFtBpWP8LBdG6eeVke5cPoDP5Ot
dlZarKrK+1UK5D0sFqC0n7h7WvmE6s8caZ5RhP2P1TvFMhrDnRw0sUn6
INFVUhxhN6/WrZ07M6G6Scht8Z9KvBqvBTRbF33FwSh0wFbfwD5b9
mP8Nal0t9s6fGl8p9gB8/3jAiN6wH6y6xzt1v16m6us7sQkyx6KFPvZwEmJ7ac
NN/JWcH1LFW6sAhsP1+meRfEOVfNetZsp2b1D9Rq2xO6X6hm0D5nHCvAv7
bf9sPs6lu1u97S2553os6R6h7Pqbagp8tuHUtV6UqYK1D80RrakfY8G86D6l
pQF66w66eR6q HK-RxQSVUJrs8BEt8Qp6sDK6pYMUmu5EatQj5JO
AEEALkgYl4vyGg22A7dPdcGrcK2rnEOUs6U5U7/5V7/5E5BYvK8nKn4X3vU4JcVbF5PQ
42c7J/7eVRAW1Feu5ArKayGuv4975XUK3AT13t0Q1BM6yV6yQblq5gSj11U1Tewd
Suy3YuynbH66Qf6P9N69ZD68hLXh68hQ68hMU7wBD600wMexMAATiU+r
RZqwen0P6yfGvsuoU3wUE4hvP3013LrAfbPK9cA57Ct1vHNNREH0K8dNplc1IIM5YHu8
QJ536/qFzKPC2Q55Dazv25QfDqy9LrTa4Uf+wsLzuJjegwPjoDdbDczT
20ToeUHfrWCh06JK8sbGgMC0EAAAYBQX7QYOAQDw1LcxyAa0bD0U4WYB
aGKACkTkdxs9/h2Fs5+hB+G8BQ90pamg0cHx1PvKekrC+RcVMpSkgmMQG5L2
H4xP3asb5PlpCwJuyxVhga4G040d5wO/jw5a7TfWtcKk68yPQe+P0U06H9GZmLsLm
mcCEnXVANPb70vQmGOoOe627U58sVazkX99d9RO85Nh9fRqFw7kKb30hXw7
TAgFjOG1ZG6uADST23FaqByfCveAYVARK2z06bNqa5350W53D31yvd
10Lk6B83Z0gg7Uktf6f2xaHlcmWf5zF1rgqSl5bh6P6BWW7rerhMna/01Qb5
YKG3qLyvca3Sl3gbogVLAzQnSNW6vVIlE28ffy/fd
ns5K
----END PGP PUBLIC KEY BLOCK----
I want to prove a message is from me

- I encrypt (lock) the message with my private key

- Anyone with the public key can use it to decrypt (unlock) the file. If it decrypts (unlocks), then it must have been encrypted (locked) by my private key and no other.

My public key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH
KozcrFpy9XoGl9232tzzXCCog3bMEoO6EOIFNf0vaC0b84jjq208nHwSLL
BZndqPcqXcn2GtizFEHJUaHUf27C05oCbxPMeshUH32kq+g6QtxM1lb3Pvp401t
1zapmdQog2H2zwBR8YFidzouertekOFrCySFZ9KMcDAeL89d4FmWnq3dvz4I2R
GYEZK5+OhbcG++rC9H6an7G5W5HOFW40U5YSZv0tjyQdFQpkr7r7uz339kHvH
Bb/7ty7mL6MBq6U2OQBDB5w7sICqT7K5bYXVUJ6oBBEAGIlbkbwWgVmFusWbIDr
m6uJstWh58G8z52CH5YJz1a61EBwE8ACAFKbVvECmYQGCMA+AVHeCwX
BwYUQ7CAf8cCggCYgFQdAIqLDE4ae9s45CWXs495+pFR+CAhCaY6gH59sW
GW8W5qkC6OYBlxq2aj3hPmynhymZmQEnr1a1KhC0rjj2b97S5/7+hEgOHrR0RMt6g
S12oEPEdI4d8Fk3d522ODWd05mWpn0OrM6y9t6F103ssowUQsQ43d3b1pt
SveW5PCaO+m+KXH9D5C5OEJIKPZ973P29nqKX175sNQ9DPCDP3dBGh8w7+eP3K7X7H
JenX0n+1337Q2Y9ctzicGbmewrHRfBU8hYRDCz0J7u5Se4hZm9HngMnt7O4D
Y+r5w3r5wMwzan2oHa9edV48/HZm5uy6C6Ih6ECtWg7pQ2g0oowze67
T6pfwwrQGmB1W1LpjF12hmbMlKZx2l8b2876zYv07FpokXQGQ7UJALuA
lwUCYcYbGgACogHw4nBHUuUjkqCwKqUvQhMBAH4AHBeAABQhCWlMeAhAABoAEJN
zX9D8b38JKlAIAJw7YhmYmS6C6MBMGt11x1DXOAb17B70WQ2Hsk4UAcEd+a
BWB4ZLcXuStaZvXxu3q3BqG9o1HMEG5KGu05JWahdz2QHczqWZjK0uJ6Jf
Bilaw4wkWvB17e4k44McKxLFStx0EA6HRLTv2X50dKivmXKcKbXcb7k1n7m
ccn1OluorDe1ebxkNy6sOlDwpk30j0/j0yF5Yu8p9oivy2v6/wQdQeHgljxv83z
9weMrUrZuUv/0PzqjUjMDj1y7t7D5R7Y5/FSFQZODA6cos+Kb0Pn7mTvYvD903
pzbv3jpe7vH3bXwZv8Y2z7T1t345sW9RMRJIAEhw4EYCAAF1TnSEALpgCQYXm
p99Hb2z8BA/+0pcxOn2bU6Ybyt047lp2p2wev3DF0SAh1VM7yXK6Ly6p93t3w
XmRJU,IweYaQ7z17mWNCNRJQ5yQ9VjzPw2jJQzTshJhK5S77ClQXXTe516eny
2nucgoj1Uv3C3ZBJcUcWes6f1X71P7v2/g6UJKmD0Pb82btpnHnMAYK
401lHb1fLY5gnmwozvJzHcHdCOP0zem1eMeei6ekh6R83hSWsk588tK7+sk/Z
H3ECB8mpR9mwey6gG6PwKwYcV9WWM80B8RtRgKwpXw8L3B8G466YPE5yG4Kd
3lKrrlxK+L1KUD5fsoCOn7nhw77y7VmW68eCzjz5hSPR2P2T1FvMpydOrkVbosoWus6
INVFUSXm+dZytBr0k7O166BelSCCHT8QD9bYbTfFw5BflfBwlyDh94
np6DNA1ons784gwp98BZJZiJnWmaX6x3y1zv1rsnQ6i9yKspWz2emDuJzAc
NNJ/3WChL5FkJWsOAsp1z+1meP6p9l60wNepetzbp72b906qXs6Nk0m0hLahnV7
Fs6bupUl6u2G7S5sOx1R6h9Qbug3aq8po0h9vW9vV9YDQ1Bh9Akyk6gqY9d8tca
P/FJwArAwP8WqwqFnpUH9QXusUXE83Y8KpR9j0P6K10Y5m5sQAx8LYC5o0x
AaIyLyrXVyyG2zA7DpGdcRMhhoQ0USUltV/7E5SyBKYh9KN4Kz3JL+3vCQ40GcpQ
34c7/5vRRV1891ttKgrLscv047T1XKUS43T1oE0lx8t06Gq6o8q0Sg11Z1UwTdf
Suyoxl4egq7wF0lN6JZEnaJxPdx4kUXQ5Jn8H69MsU0D0006wHMAAT2h+R
R2w6o6pPjLyg3v3rUwU4wPty3D1EAL4fbp/NaCtu5vURHRNDOQWkJcMi5MSuH
QB3Q63/eXcP2Q5SSZMszsF25pq2yQpDLHip8u7SfJxJ5wqPj0D0cbC7F
2O3sX7HHkZ70QDH2lE8b91bWOGAEO4AHAY8QYAXQAQAwLJYUxhB4DX2D1WYB
AaGACRC8Tdxs89Z59+bH798Qpimgko5fHx51VPkkZt3w+Wvm/SkvEPgMQZC2Z
4Hx3apsR7LpCrguUw9yH5aG4100dW05vS/Daw7rZCnKed6rYp0g/DUO6Hd5ZSUJn
mCnqan8Pn8boF2/xmGo4Gx627U85vxQaAXDy8R86on5Kh7aHzK2bo3hw
TgA+JQ1GQASuA6uADST231Faqbzyfey5AVK&qro20BQnbaNqI35b0315syed
ll0bX83J/Rogg7hU7K6F2xzClicmUw5F:XFrh75ClSShKhsPlBsbWwvHef5mna/aQab
XYQgZiFqhyc4As35IgbqgVLAzqN95PwHVrVE28fYt/ed
ns4F
-----END PGP PUBLIC KEY BLOCK-----
I want to send Bob a message that no one else can read.

- I encrypt (lock) the message with Bob's public key.
- Only Bob has his private key, so only Bob can decrypt (unlock) the message.

My public key:

Version: GnuPG v2

mQENBFHMcgABCAC98Y9YDQ2L3YhVi41eHIn6uALqMg1p+S0u7CUEvJ1z0x0AUXH Key fingerprint: 9X0g8I@3932t3xZC0g3m3eMeED0e0INfoxOcA3B4jwq0j1NhWw5L 8ZdnpCgIpCnx2G2iAFe1hj72OFC0bC6PmesxHuZikhe+e6datm1x1Bp4O10 1zqsd0MqH0g2Hx2w38RHYfDq3ouetekCtLvCvSy7F9KmA1eB9H14fnw SQhZdZ 2YXE25+x8CBG++cR9H6an7EG9WHOFWR40uSYUz08revQFqZkktEu7u2339wYH H/0b7/yU7MXG6Q0UZ2D5w57I8Hq7KxYXUyJoDABAEEEAGb0lhbkWgVnFMWUHd zdmfuasVh0g2su5z52z5y3y1z3JAdr3ewE2ACKFAYyYQyECCyM22QAHAVccw kVuHx2G8Yy1t2K9cYvXAgcFGdGdAELQCyZ4C2Tb8WZyC3R2Jn0K+0CA6CX9QW GH6H8kx46BlyOq3zWp3q3HptmhYznqj61a1C3Krdj2bQ7S57Eg0H0RPI0Qf56 S12sEj6a1A6Kkz32Gd2wF1J0WpYnq6MeGtb9tVf1S9wvU9q3p3Dr1b5b3f sWtC3vXvT+KHDS0C1T77P2P9r-q7X1L2xAn0Q3F0c7d0arrrh+V+yik3y+77z 7mAzpX0o+11332Q2Y3tC8gbevYwKmHR8B1Yj3cO7q7USe5F7Hz4mGzn6mgOutQ4 D13G5w5f3Wv2sra39e9d9v48vWvnsns89YHF35UeC30C3c2F2PqQ9o0we2Z 6l76t0pG8dYJb1LWjY1pPxfh2bmkayX2a1XbZyYDw7Pw2Ppok3XgQ3AaJmLw lvWJJCYYkAcG6hWlbhBnUAgkqC1wqVagMAb4AhaABE+34WfAMCnMmAbBkAoAE2N z38800j42uIAwunYfm3yR62EO0MbGm8Xr0uDKAcP1t7BO7WQ20h6QACe1k-a B9Y1B1aSu1lztuyxf1x3q926eR6y1y6w1H3g5tu0W1w06v2Bf5h9aQ9fLl75I5f B7amaw0KWoi8e44akMcK5xC8FBea0eHI6L2v1x50DvKmVlnKk0ebtb7k7m Lcn07olb19eD0XyozBsnVw/pkDj00j/EStW7e90y3zy7wF3b5Ig6R3Ez3YwXmxRjuw1xz71m3CHG0R5yqV/vj/1G7J7+5Gq3jxkh5h6/7E9QX7tKxMEny 2nudcji01v2sC3BZJecuwfes1x7FnP2+6gUk6MDFP3s2bbyrHmnywAYL 41qHFB1Y5Jgnw0z29h0C9h902m1eMeIIeKv9388n13BwkS6PK7S+rZk17/C E2BlUp6h96v8Gw3pW2vTuCW10MB905vfa8c2pWBLA9G616eYKc0Fy7G9fJ1d 3LSz6Eny9xUK0y1D5s6HwOJ7nmg07vH7vWmF66eac2h9SRIIP2WTFyMdirKYbVosuoO uNFvU3h8m9Zytp1078e6i6C87k7xZbyBjrHFtBSBPF2DSbIwEFw9YI94 p3pSNcI6o3GlG7a2D98G2Z8Juxy9MN6y6x2z1vmonsu9y8y5SPF2WPE2IwUmJaC NN/3WchHFLkQDas0hps+1meF0D0wNcetp2zbj9T9psxG6hOmoD3nhLcrAV97 Fb5psUju1bAY215S0x6386HqfE9abapud8ptuhHV2wRyQID0yAK6yEYQ0DcBta P7/F6L0rO42nHw6fesp69-RXsQVaYsUxvSYFmbrz6D6M5KPMl5m5u5s24UO n11A1YAYfL7wF2eX7dDj54hRncm3Q0o5UI9H7V3S55BO1Enk4x3xKvLcSF5pOQ 42Z7/MT%wRAZe11b4sboCCvL9X1USK4A3t01e6Bm66yq6bqQ9S5112U7vCw SuyS14ly093FqRnDP06Z1enZlhjuxWhh08h8mMUU/0oD0owm9A0M4T1IA+R R2w6q6nppj5GxhJ1xUwU4f33y4T51EFA47Y5s/Nac5tu7HWHNDWNPIClHSm5eHuB Q3Oz7ecN0PZQS5wD22fz5f2qGyDypqLUATy7p+wsUJl4jItqDIP0Dcb2 tZCI3DNhYmZGl2PIkZXLGj5OAEMQ4AAYBZQYAOA4b0UcL8CpxyAbQJAUvJWY gaAKRCC6sdx79Zf5h+8b9kqfmg6Q0Hm141VXfKewk9L+VwMsPkEgMQ6LS2 x4H3asIapdLpc977wuyHm4A400dw50jYv/a7TwFZrCndY6Pp04U0UH69SDUZjM mCn3gEPMV16o_HSfumO6ex275nU5aXbA80n8B0tKbQmXkEm3C30Dn0Wd TAqJOGZIJE6uADST231QaBfzyfE5AVkR0w2Bjnaq35vD05315yvd Ro8b3x7qH87Uk61j2vZnIcwmUf5x7F5r7C5GbosHmR6BwWvHeRf1a/nm3qab YKGMqBvuyja53s1gbogVLA0zNS5WHBvVEE28Y/yE/d n=SFK -----END PGP PUBLIC KEY BLOCK-----
If I do both of those at the same time I can prove that only I could have sent the message and that only Bob can read it.

My public key

```
BEGIN PGP PUBLIC KEY BLOCK
Version: GnuPG v2
mQENBFHMcgABCAC9WYQDO6ZL2WY4ehhEnGuuLqMgI3+5UHlCEvLUr2qzoXAUHX
Ko3kHpfh9X0kGh3232trZXCg3mKSeoOeO6I6Gf0vaC8d4wpo3th6Nwh5Sl
2B2npQioCpinXH2geeFihUah7FC2oSwCbgPnMesUh4Zihkg+6g3atm1l2BlP401Ot
1azPmOGbK2H2xw28R3Yflid2ouetekOfLcyC79fKdMA1eB8HR4mWvZQHd2R
GYE2x5+M8ckGB++cR9H6an7E5GWHOFW40U52S0rveQfQpK7r7u3z39H96H0
B/7n/7v55GQbu02ZBDSSwI7QToHqnYY3vdU00ABEAOOA6l0bHg6VWqFshWidOx
dmfa8aVnHq6b252ZC5ETHj1z36a61TBE6eEACAFKRYEQGCMqCZmATAhWcK
BYB2A2YCAIYcqlCggFGDA6Dr3kEn0QxGACRC5vdw9xFZG+CAACuhkpe3qzw
GWH8k8G4Cj36BY2q3PnhMyznQm6qv13x1C0r1r2j/B5/755+5EmGh0RlP0fK6
51380t6e618K3k3g2dW2D6YtwbPqyM6bGtvF1630v2eQpe3k3d3b1Pst
sv3x+Eh3Kl56Kc07F52fppqX7v2S1/nKHmQOpC5rQ07db4+P5ypKXKyzaf
JXnAPX0+3l33ZQY9ec7iy2ebywenHMrP27BYCZd7r9XSe7F2zhMsQm7OZw2
Y6z5r5fBlFvna2D3hj56eV94bW4w5uBfRHY8SH50Nh3cOYc2CPyEq2010w6Z
67GdirwCpZG1L1wP1wF2h bundles>KaBZa2kt4B7d5J3WZCfuV7P0kik1qdTAJ5ALb
Iw7UCVYBlcAgCWhgA1HwBHUnAGkGwCkwAqWgMBA4hBAeABc7AMCwMembAAkOaEO1N
zG6s9d9sR0GwA1Wfr1Yrmk56sElGBGMM7x1DOKAc1lR7F0V02HsIshuUCec+a
BXY1A7Qashatze3xa1q3meC2Oz1ynmG5E6GKx30WwHbst2iZHcExpN1L3D75SM
BilawwOKVoW/b8ee4kAaxkCJHsF8Bf6eAHRl2sV152DikVnKcocKtu87b1nLKh
m.c/L1Q6bV10eLsnoB3nO/yKp03GmIO+EY5Yv90olv2yQa6w/6g59eh1xLxye9do
9we2u5yu/+kP8z4j1iM6Dc0u7y17qS5FI7FO0D4Nac3c0wNm7uU0y08u2h
pzbv3g7eVHwRrWbYvZ2T13t5SNW3M0JAHwe6We6CAEAYAF1SpaGCGK3Wv
p99hBT288A+0OCh2c2BnBh5by0+41ettP32we1vDf5s1Vfh7yXYD6yypf3t3w
XmuFR1LweрюzX1NebWNcROQ3h2vB6vWjepjl01u1+2C5hj3k7KHeX7CQDXTrk8Eny
2nucdnCg02v3C8Zj2kCcUe6wes11x1rPf/17v6g3UHeMDPsw2bttrh3nN0YkyKML
140D0HQ1lyfNgw283h3sbcH9s0Qe2m1eM1e4tetkHe639s3Bwsk8fFt3t12
L+3EBl8B8Mfr9B96rGAPwpwKCU6Y1MB0sRX/8FbAyTWL8C6q06c5KdE137G7
ZiarxK+m1/KD5sfolGChO7nwhwyy7vm61E8sca3h3RIP2F1vMyd rocketBvwosun6
Ivuf1sNe3h=Ztv5hBpT0786ebGcSHTB5KYb7rHhtBt8Tf3w5f7b81f9wy6wDy94
n/PicsnorC365b11988p98b119B22/najaW665/zxt111vmm7nuq3ykypf2w3mU1ajc
NN/3jWclhFLwKbDAs1hp+1meP30oUletz2p7b9a9q3xkD5Oh3sOmcHahC9V
9sFlpsuug3LasY5z135s2r6q89e9bg789uUfthiuVq39X8DQ10kkaGq6m8Dc7u
ysuZ/Cw3j82d86fpq4N-H2s5USvUwe3EBNwrdp591M3K5Ymmsv3K30Uj3xy
AeALayYyGyZ2aZtpDpcgr6hMnoQO5U5Vp7/53S5ByKbn4K3nx+V1eC5pfspQq
43z7c/7WVRA1wB95aHRGcVeV947TSJUK3AET1e0bxM6qG6bqOJ23014
7wyfSdf62p2FQpND99/Ze7knXQPHd1whXMHH1mU07vqD050mO2x9mATk1h+R
2qwe6ofyP56Ur3iuuWw5eh4T4D1eAFXbkoP+nac5tuVhNRDNWpPcHs5M8HUb
QJbabs/t/ExC2fPQ2SSq52dav7FZQgyDPw1ATux+wUsLznJUwrgPjROdC2Z
TPNv7Dh8nM06ZgKX8ki8sL9bQ7eA8QHv8uYQbHJX6q9RqW2oIEIu1jUkPW
Kx04F6PbuG6v3bUv9932J1g30v309E15K4tv8Vw9gY422DswwyO53w/3lF93
mCenZ8PQx0Fbo/mGmQ0o0e627U56vqXAvX7HoB0tNkQfPkwX3Bd02kwv
TggAFljQGz1e6uADsT321fdqBzfyS5fASVRzdook2oIbqan35sQ30D515syvd
120b837/II07q7Uk6tf2ZvICXICMwLuW5FYrFl5cSb scratchingHetP6bWwHfWentRja/a
QmAY1fIq9yhauAS3jIgagcVLv6jNs8WvBf88y4f/Ed
ns5K

-----END PGP PUBLIC KEY BLOCK-----
But we still have a problem:

All that assumes that we know which key goes with which person (2).
How do we solve the identity problem?

Idea: Have the humans do the linking of identity to cryptographic keys.
We could post the public key somewhere highly public and verifiable it came from us.

Adobe Product Security Incident Response Team (PSIRT) Blog

Working to help protect customers from vulnerabilities in Adobe software. Contact us at PSIRT(at)adobe(dot)com.

PSIRT PGP Key (0x33E9E596)

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

Photo credit: Juho Nurminen
@jupenur
Other people can then compare the keys on their computers to the highly visible copy.

Photo credit: Juho Nurminen @jupenur
Though we must be careful to post ONLY the public key...
Nice idea, but it does not scale.

Also a chicken-and-egg problem. How do we find a place guaranteed to be from us without using cryptography?
Idea 2: What if everyone did a few verifications. We could slowly build a web of verifications like:

Alice verified Bob’s key
Bob verified Charlie’s key
so
Alice can trust Charlie’s key
Alice hand verifies that Bob’s public key really does belong to Bob. Then Alice “signs” the key by encrypting it with her private key. Now anyone that has hand verified Alice’s key, can also trust Bob’s key (if they trust Alice to do verifications).

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

m2ENBFHMcgABCAAC9WYY/IXYYLOZVHynenHN6u6Qmp3G+5O+Sv2vEtZnizwNvMw/X
KoaHeF/y9XoGh8i933t2zXyCQ3/orQ6oEo60EFGnoFozcB84jwpo08BNWn5/L
2BznpoCipxcn7GzioFe/1Uah727C0OcBcrPmEshuPH2zKir+6gZdmtr7jLby4vt5O1t
1zp86IDGedz2m6X2t8dfmYfJ2AeZzv2ktEq/LCq/zf9KdAhJe8B9hr3iQw2zqA4Z
GYE+5c9GCGb++c+94H6an7EG4WHOFWF4R0wY5Z0nFyqYFkk7o7u333rwhHb
Bt/h+7Yc6MdBQ0UOZ2B05wJ7iQh7qKXtVrsUdA8EBAAAOGi5tW1/gmgvFmWuWHbdX
dm/fUuV8h2uSqi5ZC52CH5YzA1v6A6T8EeE4WAC4AplYQeG5COm3AYA4V0CChwK
Bw4CAmFkCKCQAcog5FgDgAD3e8oLXQK6ACRSG1xwY9M9FgCACHukFQr89
GW8H/kqG4b6Y0bJoz3qJ3PHmyznMZePwJ1xzDhRj2b75T7/gEtPQh0R0jw1f
Z52oEPe6Af8ki3G2d2武P0w+8NqOYb6H8GeF16O2v8eQ2G3eb318
SpwrEFabi7+KtH3JQFt7ZlPBqy9kylF/sLdkQbn0Dq87p8hBb+FQ7yeha
JaxPn6+u13+13tJ2Y9eti\g7bne\w\MhZP2YJZPCd6y7uSe5F6rH5mgMqGdLZ4
Y1/o5w6mffim20w2zdeRe9Y/vzr5w3Yv8Hw550Bh5GvctfC2P9z820iiwz26T
ispwrCwS+1R1ly1P6v2hbnmZ5A2zg4U8ZyWZysU2l9/PokinKQ2B5TAbHnl
Iw/LVhC4Y/eZacOGhW8hB5HHnUQgKawQWagMBAH4BAEQBxCBMeHMeAABoEOJN2
z6x3Bh5bJLJW1/77rYfrym56C50WBGmT5x1DKoATC517B7W0OQksHqOvEdc+a
XBYCIJvIstu6xz13q3mE6Lv1G5Kv10Wh6bQzHqJqUW7lO5J
BibawOvw0vi8/e44ak4xMcKfGB5x0eA6HRLk2x1V50DvknVkk6ux7mb7knL
mCnL/7JOrb1d/1DeylyuNzbOrvJ8pZ0j0yF5yEyKQ9yol9y2y6wQBeg8Lx/yeln5O
9weBuUztr/vbP8zqLjMD/pB7silY/5Y9FwDw5v4+oCzw/HbUny09
pe3v3e7vHM23bYVZ2/7t13T45VWRMOJHJhawEwEC/CAY1fntnSeApCgKxQyMk
p9898b288+/Z0+c8n2bUB8bWy8tP17Pz21wee/DF5a8c1v7m7X56y69P3Tt3w
xmFJruJwEtweZxJNe/WCNQ/rbnpQvWyv7Pjw2+3Qh3ijhKu57E7CqQXTRD26Gn
2num/c0i2v/C3Bi2Cjucw6esLw1xPj/vP2+6gUWkm3OPD588zbtbpmHnAMYK
41D0BHF1sY5gn9z2z610H90z2m1eMe1e4KHv636Bw356bK87tS2Z/bL
vC1EB8BMr98Wg9Yp36W9wvV6Ow3aVw5bS4T0B3hkk89ATk79wPc9/a69
Xy3zB/h8608W0Ip6+6Wl9a1Fh0Z8/gPeFAP42zE883d4QYiq
Ziark84+K1UKD55fOGcn7nvn7vwh7/VYm6E8cazh5gR/P2TP15vMydirk0wVwv3us
rNVrLks/Hzn429P0T708b6iGec6SH/t8B8qyhrjBts708wv9bfwv9f9d4
pmPlCnQori6gJlTq9gBByBZJ/x7V7maN3s3s11x1Jvd5sU8yK5Wn2c6cEwXy4f
NN/3Wch6lFWk7Dx3as6hPx+1mF10QD0vfWvetz2Pb7A2p6X0O/Hk0Mh9vLAVj9
yFb8s0j/9piY652sz6x36Hq6Hq0gE9atd6Phu7tvHvwVrYXQzYh4dKqk9lyr6g9mR9bChe
P/Fv5eX2Gmp90H6w66Fb3KbRQs5Vrsu88yX5E6e5g/9E4Y/mkMYSM5/uaO/E המס
AeAA5/mhXvJQZkLyVwz7D3Dp6gCnK3Qr5UsU7/V5/7EpbYBNK4/uKnX+JLcvJFspqP
Jc4z7J/vRVn1/hA6k5v4/3T0KIU3X31eO6tB6nFgb5Q1s57S12n7T1dWf
tSzu5y7w/5fEp6N9/s3Enh3JxvU/L1XGZ8HrM+U/Qt6x3Wt8q986mX4/QeLX7X
R2qwe6oNpq5j/GvzurUwV4ePtyf1DeI3FLWb6/7bNc+5UH9NWDNpWLPcM5b93
QzBO36tEzC2Pv5QwS5Dzazf25pQx7yBoPlAtA7P+w3sUZiJ5wQIOPDc0F
2T9vNhrMtdZGQ2eBLeEz8gB6gBdACEA9AYXXbQYQAqAeLwLCsxyzAboALJUYYB
GAAKRCG7Iuc9Zh7FS5Hb/9B0qIgMg0cHXb1u0/nKeVw0/6V1mGqJQZ2
H4Xp3asf5PcF7yUwVYhM6400d/sjv5/dataW7rnZcKd8ypk/P0u80H69DZoMm
mC5qFVY7b+ybt0/vg09u0n6o627/U56sRaqXwXXDkRhB0IRO/kFqXw2z30hkw0
TgAfQOG/49oEs6AAtD3231qFzbyFe5VAVKxR0v08bN6Aq353W08515yvd0
IlJ8pa8/30eg7/7kU7f2/aX2LzcUMw5xK5FrRg3CklsA/sPiO65hVw7HeHrnA/\nabl/YcGZ3v9hycsA51j3gog1vLDrZoNSW/5hp8v7ZB28yf/Ed
n=xSK
-----END PGP PUBLIC KEY BLOCK-----
```
Wonderful idea in theory. But verifying those long keys is hard… also I don’t actually trust most of you to do a thorough job of it…. 
Idea 3: What if a couple of trusted groups did the verifications. Then they could have high standards and everyone could just trust them.
Certificate Authorities

- A certificate authority verifies some properties of a person/organization and issues a “certificate” signed by their private key.
- Certificates can be quite detailed about what has been verified, and what they have been verified to do.
Certificate Authorities are used by browsers to verify identity.
You can see lots of details about any encrypted connection.
But now don’t we just have the same problem again?

How does the browser know which Certificate Authorities to trust?
Clearly some Certificate Authorities are trusted and some are not.
Errors on student.inf.ed.ac.uk are a bit easier to understand though, identity information is missing...
This site is “self signed” which means that the University created its own Certificate Authority and used it to sign all the sites keys.

Why? It costs money to get a signed certificate.
DICE machines will never give you an error on student.inf.ed.ac.uk but your personal laptop will.

What is the difference?
Your operating system and your browser both maintain lists of Certificate Authorities that they trust.

These lists differ between operating systems, browsers, and organizations.
Each organization makes its own trust decisions about Certificate Authorities.

Google to Symantec: We don't trust you anymore

Admins need to consider whether they still want to use Symantec after its repeated mistakes with issuing TLS certificates.

Security teams, network administrators, and operations teams have busy days ahead. Google’s Chrome development team is fed up with Symantec as a certificate authority and has announced plans to no longer trust current Symantec certificates.

In the past 18 months, Google has tangled repeatedly with Symantec over the way it issues transport layer security (TLS) certificates, with Symantec promising to do better. The latest incident—an investigation into 127 mis-issued certificates—ballooned into “at least 30,000, issued over a period spanning several years,” Ravi Sleevi, a software engineer on the Google
Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

Superfish may make it trivial for attackers to spoof any HTTPS website.

by Dan Goodin - Feb 19, 2015 11:30am EST
hey @Gogo, why are you issuing *.google.com certificates on your planes?
Questions?