



A Um&\$% ; Yh'6G8 | BYk 'hc'6G83 | GYUfW '6G8 | Gi Va]h'BYk g : 5E | 7cbhUWh' l g >c]b' l g

Web Security: Encryption & Authentication

by Paul Weinstein <pdw@weinstein.org>

GG@z'XYj Y'cdYX'VmBYhgWdY'7ca a i b]WWh]cbgž'UbX'H@Gž' h\Y'cdYb!ghUbXUfX'fYd'UW'a Ybh'Zcf'GG@z'UfY'h\Y'hk c' dfchcVt'g'h\Uh'UXX'YbWmdh]cb'UbX'Ui h\Ybh]WWh]cb'cbhc'h\Y' H7D#=#D'ghUW'"H\]g'Ufh]WY'gi a a Uf]nYg'h\Y'VUg]WWh'bWdhg' i gYX'jb'ja d'Ya Ybh]b['U'gYW fY'k YVg]hY'k]h'GG@#H@G"

GG@#H@G' \ Ug'hk c'a U]b'ZYUhi fYg. '

---7]d\Yfg/'k \]W'YbUV'Y'h\Y'YbWmdh]cb'cZXUHJ' VYhk YYb'hk c'dUfh]Yg'fU'W]Ybh'UbX'U'gYfj YfL"

---8][]hJ'7Yfh]Z]WWh]g/'k \]W' d'fcj]XY'h\Y' Ui h\Ybh]WWh]cb'cZ'h\Y'hk c'dUfh]Yg'fU'W]Ybh'UbX'U' gYfj YfL"

H\YfY'UfY'hk c'hmdYg'cZV]d\Yfg. '

---5gma a Yhf]Wf]di V'W_Ym]V]d\YfgL'

---Gma a Yhf]Wf]bYWYH_Ym]V]d\YfgL'

Gma a Yhf]W]V]d\Yfg'i gY'U'g]b['Y'_Ym]Zcf'Vch\ 'YbWmdh]b[' UbX'XYWmdh]b['XUHJ'"#b'h\]g'WUgy'ž'h\Y'YbWmdh]YX'XUHJ'g' gYW fY'cb'm]Z'h\Y'_Ym]Wb'VY'gYW fY'mX]ghf]Vi hYX'hc'Vch\ dUfh]Yg"

#b'Ugma a Yhf]WYbWmdh]cb'U'_YmidU]fž'Vt'bg]gh]b['cZU' di V'W_Ym]UbX'df]j UhY'_Ymž'g'i gYX'hc'YbWmdh]UbX'XYWmdh] XUHJ'"H\Y'di V'W_Ym]YbWmdh]gž'Vi h'W]bbch'VY'i gYX'hc' XYWmdh]'Cb'm'h\Y'df]j UhY'_Ym]Wb'XYWmdh'h\Y'XUHJ'ž'h'i g' XUHJ'YbVt'XYX'k]h'h\Y'di V'W_Ym]g'gYW fY'Ug'cb['Ug'h\Y' df]j UhY'_Ym]gh]Ung'gYW fY'"H\Y'UXj UbhU['Y'g'h\Uh'mci 'W]b'

GYUfW'

; Yh'6G8'Ghi ZZ'

See what's **NEW**

5.3



ZFY`mX]ghf]Vi hY`mci f`di V`]W_YmY`mci `Xcbfihf]g_`h`Y`
gYW`f]hmicZ`mci f`XUHJ`Ug`cb[`Ug`mci ` _YYd`mci f`df]j`UhY`
_YmigYW`fY""

I`gYX`U`cbYz`Vch`V]d`Yfg`Uj`Y`h`Y]f`g`cfhVta`]b[`g""Gma`a`Yhf]WYbVtXYX`XUHJ`W]b`VY`gYW`fY`
cb`m`gc`cb[`Ug`h`Y`_Ymi`gYX`]g`gYW`fYXz`k`\\]Y`Ugma`a`Yhf]WYbVtXYX`XUHJ`fYei`]fY`U`cb[`Yf`
dfcW]gg]b[`]h]a`Y""GG@#H@G`k`cf`g`Ufci`bX`h`YgY`]ja`]h]h]cbg`Vmi`g]b[`Vch`hmdYg`cZ`V]d`Yfgz`
Z]fghi`g]b[`Ugma`a`Yhf]W]d`Yf`hc`gYW`fY`mYI`V]Ub[`Y`h`Y`gma`a`Yhf]W`_Ymi`UbX`h`Yb`i`g]b[`Y`
gma`a`Yhf]W`_Ymi`hc`hf`UbgZ]f`h`Y`XUHJ""

5`cb[`k`]h`h`Y`hmdY`cZ`V]d`Yf`VY]b[`i`gYXz`h`Y`V]d`Yf`g]nY`cf`ghfYb[`h`U`gc`d`Um]g`U`fc`Y`]b`
gYW`fY`hf`UbgU]h]cbg""7ca`a`cb`m`Zci`bX`(\$!`UbX`)`*!V]h`k`YV`Vfck`gYfg`UfY`Vtbg]XYfYX`k`YU`
g]bW`h`YgY`_Ymig]nYg`W]b`VY`W]UW`YX`]b`U`g`cfh]h]a`Y`dYf]cX`fUddfci`]a`UhY`mcbY`k`YY`_`
i`g]b[`W`ffYbh`Vta`di`hYf`dfcW]gg]b[`dck`Yf`fH`YgY`k`YU`_Vfck`gYfg`UfY`Vta`a`cb`Xi`Y`hc`h`Y`
I`"G""fY[`i`Uh]cbg`cb`YI`dcf]h]cb`cZ`ghfcb[`YbW]mdh]cb`UbX`\\cdYz``mik`]`VYVta`Y`Ygg`
Vta`a`cb`k`]h`h`Y`fYW]bh`V]Ub[`Yg`a`UXY`Vmih`Y`I`"G"";`cj`Yfba`Ybh`E`H`Y`ghfcb[`Yfz`%&`,`!V]h`
ghfYb[`h`V]d`Yf`g]UfY`bchi`bW]UW`UV`Yz`Vi`h]bj`c]j`Y`U`Uf[`Yf`h]a`Y`UbX`fYgci`fW`Vta`a`]h]a`Ybh`
h`Uh`fYXi`W]g`h`Y`i`gYz`bYgg`cZ`h`Y`XUHJ`VY]b[`gci`[`h`f]c`f`YI`Ua`d`Y.`=Z`=YbVtXY`a`m`W]YX]h`
W]fX`i`g]b[`U`k`YU`_`V]d`Yf`gca`YcbY`W]b`W]UW`]h]UbX`[`c`g`l`cdd]b[`k`]h`]b`U`k`YY`_`=Z`=i`gY`U`
ghfcb[`V]d`Yf`h`Y`VtghicZ`fYgci`fW]g`bY]X`hc`W]UW`h`Y`VtXY`k`ci`X`]bj`c]j`Y`a`cfY`h]a`Y`UbX`
a`cbYmi`h`Yb`h`Uh`k`\\]k`ci`X`VY`[`U]b`Z`ca`ghYU]b[`a`m`]h`Y`W]YX]h`W]fX`E`"A`cgh]GG@#H@G!`
YbUV`YX`k`YV`gYfj`Yfg`U`ck`Zcf`W`ghca`]nUh]cb`cZ`k`\\Uh`V]d`Yfg`UbX`_Ymig]nYg`W]b`UbX`W]bbch`
VY`i`gYX`k`\\]Y`U`VtbbY]h]cb`]g`a`UXY""

8][`]hJ`7Yfh]Z]W]hYg`U`ck`Ui`h`Ybh]W]h]cb`cZ`h`Y`dUfh]Yg`Yb[`U[`YX`]b`U`gYW`fY`hf`UbgU]h]cb`
H`YfY`UfY`hk`c`hmdYg`cZ`W]fh]Z]W]hYg`.

----GYfj`Yf`7Yfh]Z]W]hYg`

----7`]Ybh`7Yfh]Z]W]hYg`

6ch`hmdYg`cZ`W]fh]Z]W]hYg`UfY`]b`h`Y`L`)`\$-`Zcfa`Uh`UbX`UfY`]ggi`YX`Vm]7Yfh]Z]W]hY`5i`h`cf]h]Yg`
f]75gk`h`Uh`U]h]Ug`U`hfi`ghYX`h`fX`dUf]mz`j`Yf]Z]b[`h`Y`]XYbh]hmicZ`h`Y`Z]fgh`k`c`dUfh]Yg`"H`Y`
hmdY`cZ`W]fh]Z]W]hY`g]a`d`m]XYbh]Z]Yg`h`Y`dUf]m]b`ei`Ygh]cb`/`h`Y`W]Ybh`W]fh]Z]W]hY`]XYbh]Z]Yg`
h`Y`W]Ybh`UbX`h`Y`gYfj`Yf`W]fh]Z]W]hY`]XYbh]Z]Yg`h`Y`gYfj`Yf`7Yfh]Z]W]hYg`Vt`bh]b`gca`Y`cZ`h`Y`
Zc`ck`]b[`]bZcfa`Uh]cb`.

----5`gYf]U`bi`a`VYf`

----BUa`Y`cZ`h`Y`75`

----DYf]cX`h`Y`W]fh]Z]W]hY`]g]j`U`]X`Zcf`

----XYbh]Z]b[`]bZcfa`Uh]cb`cZ`h`Y`dUf]m]b`ei`Ygh]cb`z`gi`W]Ug`bUa`Yz`ghfYYh`UXXfYgg`UbX`#`
cf`Ya`U`]UXXfYgg`

----Gi`V`Y]V]d`Yf`g]di`V`]W`_Ymi`

5`g][bUhi fY`Zfca `h\Y`]ggi]b[`75`

K \]Y`gYfj Yf`Wfh]Z]W]hYg`UfY`fYei]fYX`]b`Ub`GG@#H@G`hfUbgUW]cbž`W]Ybh`Wfh]Z]W]hYg`UfY`bch`UbX`h\Y`gYfj Yf`W]b`i`gY`ch\Yf`Ygg`gYW`fY`a`Yh\cXgž`gi`VX`Ug`\hUW]ggž`hc`Ui`h\Ybh]W]hY`UbX`fYghf]UW]gg"

7Yfh]Z]W]hYg`W]b`VY`gY`Z`g][bYXž`Vi`h`h\Uh`W]i`gYg`a`cgh`Vfck`gYfg`hc`]ggi`Y`U`k`Ufb]b[`hc`h\Y`i`gYf`h\Uh`h\Y`Vfck`gYf`XcYgb`f]fYVt[`b]nY`h\Y`g][bYf`"A`cfY`Vt`a`a`cb`nž`g]hYg`i`gY`Wfh]Z]W]hYg`Zfca`7`]Ybh`5i`h\cf]h]Yg`f7`5gž`k` \]W`Ug`bchYX`VYZc`fY`UW]Ug`U`h`]fX`dUf]m]j`Yf]Z]b[`h\Y`]X`Ybh]m]c`Z`h\Y`Wfh]Z]W]hY`ck`bYf`"Hk`c`h`m]dYg`c`Z`Wfh]Z]W]hY`Ui`h\cf]h]Yg`]ggi`Y`X][]hU`Wfh]Z]W]hYg`.

Di`V`]W75gž`_Y`J`Yf]g][bž`H\Uk`h`cf`9ei]Z]i`ž`]g`fYVt[`b]nYX`Ug`hfi`ghYX`Vmia`cgh`k`YV`Vfck`gYfg`UbX`gYfj`Yfg`Vm]XYZ]i`h`5`Wfh]Z]W]hY`]ggi`YX`Vm]U`di`V`]W75`]g`i`gi`U`mi`gYX`k`\Yb`bc`ch\Yf`fY`Uh]cb`Yi`]ghg`VYhk`YYb`h\Y`Z]fgh]hk`c`dUf]h]Yg`

Df]j`UhY`75gž`UfY`bch`fYVt[`b]nYX`Ug`hfi`ghYXž`Vm]XYZ]i`hž`Vi`h`W]b`VY`Vt`b`Z][i`fYX`Ug`gi`VX`"I`gYX`k`\YfY`gca`Y`_]bX`c`Z`hfi`gh`fY`Uh]cb`g\]d`U`fYUX`m]Yi`]ghg`]b`Ub`Yi`W]g]j`Y`[`fci`d`gi`VX`Ug`Ub`Ya`d`cm]Y`UbX`h\Y`Ya`d`cm]f`":`cf`Yi`Ua`d`Yž`U`Vt`a`d`Ub]m]W]b`gYhi`d`U`df]j`UhY`75`hc`Ui`h\Ybh]W]hY`UW]gg`hc`Vt`a`d`Ub]m]b`Zc`fa`Uh]cb`

I`g]b[`U`c`Z`h\]g`]b`Zc`fa`Uh]cb`k`Y`W]b`gY`Y`\`ck`U`hfi`ghYXž`gYW`fY`hfUbgUW]cb`W]b`hU`_Y`d`UW`i`g]b[`GG@#H@G"

%`H\Y`W]Ybh`fYei`Yghg`U`gYW`fY`hfUbgUW]cb`fM]m]UW]gg]b[`U`I`F`@`k`]h`\`h`d`g`UbX`Y`hg`h\Y`gYfj`Yf`_`bck`k`\`Uh`Vd`\`Yfg`UbX`_`Ym]g]nYg`]h`W]b`\`UbX`Y"

&`H\Y`gYfj`Yf`gYbXg`h\Y`fYei`YghYX`gYfj`Yf`Wfh]Z]W]hYž`k`\]W`k`\]W`Vt`b]U]bg`h\Y`gYfj`Yf]g`di`V`]W`_`Ym]b`U`d`UW`_`U[`Y`h\Uh`\`Ug`VYYb`Yb`W]m]d]hYX`Vm]U`75`"H\Y`75`]g`U`hfi`ghYX`h\]fX`dUf]mž`"gca`Ycb`Y`k`\`cgY`di`V`]W`_`Ym]g`_`bck`b`Vm]h\Y`W]Ybh`"h`U`gc`gYbXg`U`]gh`c`Z`W]d`\`Yfg`UbX`_`Ym]g]nYg`]b`cf`XYf`c`Z`df]cf]m]"

`Ł`5`Ł`H\Y`W]Ybh[`YbYfUhYg`U`bYk`gma`a`Yhf]W`gYgg]cb`_`Ym]VUgYX`cb`h\Y`df]cf]m]"gh`gYbh`Vm]h\Y`gYfj`Yf"

6`Ł`H\Y`W]Ybh`U`gc`Vt`a`dUfYg`h\Y`75`h\Uh`]ggi`YX`h\Y`Wfh]Z]W]hY`hc`]hg`]gh`c`Z`hfi`ghYX`75gž`j`Yf]Z]Yg`h\Uh`h\Y`Wfh]Z]W]hY`\`Ug`bch`Yi`d]fYXž`UbX`h\Uh`h\Y`Wfh]Z]W]hY`f]g`VY]b[`i`gYX`Vm]h\Y`gYfj`Yf`h\Uh`]g`]ghYX`]b`h\Y`Wfh]Z]W]hY`f]t`cf`Yi`Ua`d`Yž`]h`Vt`a`dUfYg`h\Y`I`F`@`]hi`gYX`hc`gh]Ufh`h\Y`fYei`Ygh`k`]h`h\Y`I`F`@`h`U`f]g`]ghYX`]b`h\Y`Wfh]Z]W]hY`Ł"

(`Ł`H\Y`W]Ybh`Yb`W]m]d]hg`U`Vt`d]m]c`Z`h\Y`bYk`gYgg]cb`_`Ym]h[`YbYfUhYX`k`]h`h\Y`di`V`]W`_`Ym]c`Z`h\Y`gYfj`Yf"

)`Ł`H\Y`W]Ybh`h`Yb`gYbXg`h\Y`bYk`Yb`W]m]d]hYX`_`Ym]hc`h\Y`gYfj`Yf"

*`Ł`H\Y`gYfj`Yf`XYW]m]d]hg`h\Y`bYk`gYgg]cb`_`Ym]k`]h`]hg`ck`b`df]j`UhY`_`Ym]"

+`Ł`5`h`h`]g`dc]bž`V`ch`h\Y`W]Ybh`UbX`gYfj`Yf`\`Uj`Y`h\Y`gUa`Y`gYW`fYX`gYgg]cb`_`Ym]k`\]W`W]b`bck`VY`i`gYX`hc`Yb`W]m]d]h`UbX`XYW]m]d]h`h\Y`fYgh`c`Z`h\Y`fYei`YghYX`XUH]"=Z`h\Y`gYfj`Yf`k`]g`Yg`

hc j Yf]zmh\Y W]Ybh]hk j`bck Ug_ Zcf`h\Y W]YbhWfh]Z]WWhY"

=Z Zcf`YI Ua d`Yz`U`W ghca Yf`k]g\YX`hc`di fW UgY`gca Y]hYa g`Zfca `Ub`cb`]bY`ghcfY`k]h\`U`
WYX]h`WfXz`h\Y`W ghca Yf`_bck g`h Uh`

....H\Y`Vta a i b]W]h]cb`k]h`h\Y`ghcfY`]g`gYW fYz`gc`h Uh`bc`cbY`WUb`Vt`YVh`h\Y`
W ghca Yffg`]bZcfa Uh]cb`k \]Y`h Uh`XUH`]g`]b`hfUbg]h`

....H\Y`gYfj Yf`cb`h\Y`ch\Yf`YbXz`XYWmdh]b[`h\Y`XUH`]g`]b`ZUWh`h\Y`cb`]bY`ghcfY`z`UbX`
h\Y`W ghca Yf`]bZcfa Uh]cb`k]`]b`ZUWh`VY`i gYX`hc`dfcWgg`h\Y`cfXYf`

=b`Ubch\Yf`YI Ua d`Y`Ub`Ya d`cmY`WUb`UWV`gg`h\Y`Vt`dfcfUhY`=bfUbYh#9I hfUbYhZfca `h\Y]f`
\ca Y`cf`cZ]W`UbX`h Uh`

....H\Y`Vta a i b]W]h]cb`VYhk YYb`k]h`h\Y`Vta dUbm]g`gYW fYz`gc`h Uh`bc`cbY`WUb`Vt`YVh`
h\Y`Vta dUbm]bZcfa Uh]cb`k \]Y`]hfg`]b`hfUbg]h`

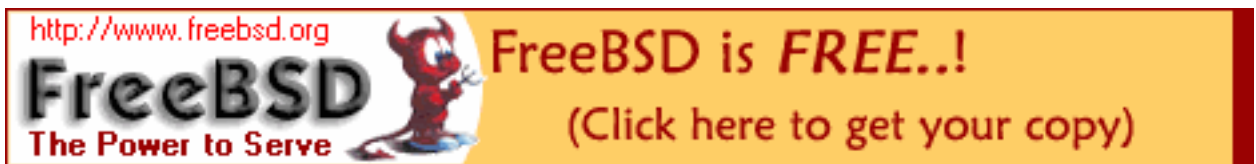
....H\Y`gYfj Yf`cb`cbY`YbX`cZXYWmdh]cb`]g`]b`ZUWh`h\Y`Vta dUbm]gYfj Yf`UbX`h\Y`
]bZcfa Uh]cb`]g`j U]X`"

....H\Y`W]Ybh`cb`h\Y`ch\Yf`YbX`cZXYWmdh]cb`]g`]b`ZUWh`Ub`Ya d`cmY`UbX`h Uh`h\Y`
]bZcfa Uh]cb`\Ug`bch`VYYb`Vta dfca]gYX`"

GG@#H@G`]g`U`dck YfZ `dfchcVt`h Uh`bch`cb`m`U`ck g`gYW fYz`YbWmdhYX`hfUbgUW]cbgž`Vi`h`
U`gc`YbUV`Yg`Ui`h`Ybh]W]h]cb`cZ`Vch`dUfh]Yg`Yb[U`[`YX`]b`h\Y`hfUbgUW]cb`":`cf`a`cfY`
]bZcfa Uh]cb`UVci`h`5dUW`Y`UbX`GG@#H@G`h`U`_`U``cc`_`Uh`"

FYZfYbWg.`

9b[Y`gWU`z`FU`Z`I`gYf`A`Ubi`U`a`cXSgg`J`Yfg]cb`&`,` '\$`>Ub`&\$`\$%`[kkk`"a`cXgg`"cf`\[`#`
XcVg`#&`,`](#)`



5i`h`cf`a`U]b]U]bg`U`Vt`dmf][`hg`cb`h`]g`Ufh]WY`
=a`U`[`Yg`UbX`Urci`h`7cdfm][`h`¥`%`-`,`!`&\$`\$`(`8`°`a`cb`BYk`g`5`F][`hg`FYgYfj`YX`"