# Final:

1. Discuss the security strength for Project part 1 using a table.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| RSA | RSA equivalent symmetric key size | AES key | IV | Key wrap key | Key wrap key IV | Total |
| 1024 | 80 | 128 | 96 | 128 | 96 | 80 |
| 80 | 256 | 96 | 256 | 96 | 80 |
| 2048 | 112 | 128 | 96 | 128 | 96 | 112 |
| 112 | 256 | 96 | 256 | 96 | 112 |
| 4096 | 192 | 128 | 96 | 128 | 96 | 192 |
| 192 | 256 | 96 | 256 | 96 | 192 |

1. Discuss the security strength for Project part 2 using a table.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ECDH | ECDH equivalent symmetric key length | Private key length | Public key length | AES | IV | Key wrap key | Key wrap IV | Total |
| P-256 | 128 | 536 | 728 | 128 | 96 | 128 | 96 | 128 |
| 128 | 536 | 728 | 256 | 96 | 256 | 96 | 128 |
| P-384 | 192 | 640 | 960 | 128 | 96 | 128 | 96 | 192 |
| 192 | 640 | 960 | 256 | 96 | 256 | 96 | 192 |
| P-521 | 256 | 784 | 1264 | 128 | 96 | 128 | 96 | 224 |
| 256 | 784 | 1264 | 256 | 96 | 256 | 96 | 256 |
| K-571 | 256+ | 832 | 1360 | 128 | 96 | 128 | 96 | 224 |
| 256+ | 832 | 1360 | 256 | 96 | 256 | 96 | 352 |

1. Discuss the security strength for Project part 3 using a table. Create a table to include all input parameters.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Master key | Password equivalent symmetric key length | salt | Key for salt | IV for salt | AES key | IV | Key wrap key | Key wrap IV | Total |
| 128 | 20 | 512 | 128 | 96 | 128 | 96 | 128 | 96 | 224 |
| 20 | 512 | 256 | 96 | 256 | 96 | 256 | 96 | 224 |
| 192 | 20 | 512 | 128 | 96 | 128 | 96 | 128 | 96 | 224 |
| 20 | 512 | 256 | 96 | 256 | 96 | 256 | 96 | 288 |
| 256 | 20 | 512 | 128 | 96 | 128 | 96 | 128 | 96 | 224 |
| 20 | 512 | 256 | 96 | 256 | 96 | 256 | 96 | 352 |

1. Compare the ECDSA and RSA-DSA speed for signing plain.txt for the same strength.

|  |  |  |  |
| --- | --- | --- | --- |
| ECDSA Algorithm | Signing Time | RSA-DSA Algorithm | Signing Time |
| B163 | 6003990 | 1024 | 1401066 |
| K163 | 6024081 |
| B233 | 9117135 | 2240 | 10321490 |
| K233 | 8196979 |
| B283 | 15353969 | 3072 | 24762815 |
| K283 | 17038535 |  |  |
| B409 | 19860931 | 7680 | 349283305 |
| K409 | 20751470 |  |  |

1. Compare ECDH and DH speed for generating a shared secret.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ECDH Algorithm | Time(nanoseconds) | DH Algorithm | Time(nanoseconds) | DH Algorithm | Time(nanoseconds) |
| P256 | 1386584 | 1024 | 768422 | 2048 | 3587121 |
| P224 | 1149974 | 768422 | 3587121 |
| P384 | 1959962 | 768422 | 3587121 |
| P521 | 2636390 | 768422 | 3587121 |
| K571 | 50733877 | 768422 | 3587121 |
| B571 | 61049732 | 768422 | 3587121 |
| K233 | 2776340 | 768422 | 3587121 |

1. (bonus) Password cracking against Windows 7.