Experiments with DSA

Daniel Bleichenbacher

Crypto 2005

DSA signatures

- p,q primes, q divides $p-1$.
- g generator of order q modulo p.
- Signing a message m:

  Randomly choose $0 < k < q$,

  $r = (g^k \bmod p) \bmod q$,

  $s = k^{-1}(\text{SHA-1}(m) + xr) \bmod q$,

  Signature of m is (r, s).

Observation: Partial information about k leaks x.

How much information is enough?

Previous experimental results

- Howgrave-Graham, Smart [1999]: 8 bits per sig.
- Nguyen, Shparlinski [2000]: 3 bits per sig.

  Can we do better?

New results

Hardware: 3 GHz Pentium 4, 1 GByte RAM (+ HD)

bits	# of tuples	time	bits recovered
2	2^{16}	4 min	25
2	2^{13}	27 min	31
2	2^{12}	55 min	31
2	2^{10}	6.5 h	33
2	2^{9}	14 h	35
1	2^{24}	130 h	38

E.g., repeat to get bits of xv for some v or . . .

Conclusion

DSA implementations that leak 1 bit of each k are insecure:

AT&T cryptolib, Gnu Crypto,Gnu Java classpath.

Timing attacks that are able to measure the length or hamming weight of k might work.