$D_6 = \{1, 47521, 47520, 99906, 52386, 52387\}$

and $e^{-1}r = (16646)^{-1} \cdot 83261 = 96684 \cdot 83261 \equiv 99906 \bmod p$, hence $i = 3$ and $k = 2990 + 3 \cdot 16651 \equiv 52943 \bmod p$. The forward search consists of the precomputation of the sets D_f. When a cipher is received, a single modular exponentiation is required to compute e^{-1} followed by one modular product and a table lookup to determine i and hence k. This provides a very efficient decoding scheme for the subliminal channel.

We have seen that if the user's secret key is $x = 3338$ the subliminal message is directly recoverable without forward search, while if $x = 3339$ there are six possible values for k—but that the equivocation can be resolved by a forward search to identify the one that generates the known cipher, r. If $x = 3340$, however, $f = 16651$ so that the forward search would have to be carried out in a set of size 16551. Although this is computationally feasible for such a small example, it illustrates the infeasibility of recovering the subliminal message when f is a large divisor of p-1 for realistic sized primes, p, even though the message could be concealed and communicated in the subliminal channel. The reader may have guessed that our initial "random" choice of $x = 3338$ was not entirely random. In fact, it was chosen to illustrate the different levels of computational difficulty that can be involved in carrying out a forward search for keys that are very nearly the same. Table I summarizes this dramatically. The message (NOT SEEING IS BELIEVING), the modulus (99907) and the primitive element (14) are fixed. The secret key, x, and parameters dependent on x change. Since r is a function of only fixed elements, it is also fixed at $r = 83261$ in all five cases.

Table I.

x	3338	3339	3340	3341	3342
y	97799	70395	86367	10254	43649
s	66281	41466	16551	91742	66927
$f = (s, p-1)$	1	6	16551	2	3

The broadband subliminal channel in the El Gamal DSS has several deficiencies: some serious and some of only academic concern. The signature $(\cdot; r, s)$ consists of 2ℓ bits, $\ell = \lceil \log_2 p \rceil$, the equivocation of ℓ of which is "used up" to provide a security of $2^{-\ell}$ against forgery, alteration or transplantation of the signature. The remaining ℓ bits are potentially available for subliminal communications, however as we've seen, only $\log_2(\varphi(p-1))$ of these can be used. This