Negotiated Finite-Field DHE groups

Group Choices

- lowest size: 2048 vs 2432?
- total number: 4 or 5 -- drop 6144?

Indication of Client Support

- range of NamedCurves set aside for FFDHE -- high byte 0x01
- presence of FFDHE value in Supported Groups + FFDHE ciphersuite

Indication of Server non-selection

- decided we don't need indication of server support if the server doesn't choose FFDHE at all.

Indication of Server Selection

either:

- FFDHEKeyExchange instead of ServerKeyExchange
  - signed message is distinct from DHParams
  - (still) not including the rest of the handshake

or:

- use normal ServerKeyExchange
  - larger message (because of inclusion of modulus)
  - simpler to implement
  - still needs to ship public share and signature

Alert Details

- what alert should the client send if the ServerDHParams signature doesn't validate?
- what alert should the client send if `dh_Ys <= 1 or dh_Ys >= dh_p - 1` ? (and vice versa for the server about dh_Yc?) (using `handshake_failure(40)`, seems wrong)
- what alert should the client send if it decides to terminate the connection due to receiving a custom group?

Other issues?

- Last Call?