Le chiffrement ElGamal (1984) est une variante du protocole Diffie-Hellman qui repose sur le problème du logarithme discret.

Soit p un nombre premier et g un élément primitif de Z/pZ. Le destinataire B dispose

-d’une clé privée s qui appartient à l’ensemble {1,…,p-1} ;

-d’une clé publique égale à g^s mod p.

La sécurité repose sur le fait qu’il est « difficile » de calculer s à partir de g^s dans Z/pZ. Ainsi la connaissance de la clé publique de B ne permet pas d’obtenir sa clé privée.

Lorsque A veut transmettre un message chiffré à B, il doit

-choisir un aléa k dans {1,…,p-1} ;

-calculer la clé de session K par (g^s)^k ;

-chiffrer son message M à l’aide d’un algorithme symétrique quelconque (DES, AES, etc.) pour obtenir le cryptogramme C. Dans la présentation originale de ce système, le message m était un élément de Z/pZ et le chiffrement consistait simplement en une multiplication par K modulo p.

-transmettre le couple (g^k,C). La quantité g^k est l’entête du cryptogramme.

Lorsque B reçoit (g^k,C), il calcule la clé de session K par K=(g^k)^s grâce à l’entête et sa clé privée, puis il déchiffre C à l’aide de la clé K.