Rolling Encryption Key Mismatch Between IDP and CTS

- **Problem**
  In the early AM on 10/1/2010, all users experienced errors when attempting to sign into any UCLA Shibboleth enabled applications. The error affected all campus applications that use Shibboleth SSO. Problem started at 12:00am and lasted for about two and a half hours.

  | **Update**: This issue was fixed on 10/1/2010 at 2:35am.

- **Cause**
  Shibboleth SSO system, also known as IdP (Identity Provider) service uses Authentication service hosted at CTS. When a user visits a protected resource he/she is redirected to IdP for authentication. IdP forwards the request to CTS via browser post. CTS collects login credentials, authenticates user and returns to IdP.

  Data packet between IdP & CTS Authn services is encrypted to prevent man-in-the-middle attack. We rotate the encryption keys periodically to reduce the risk of brute force attack. At 12:00am on 10/1, IdP at AIS and the Authn service at CTS rolled over to a new key. However, it turns out there was a mismatch in the October key pair, resulting in the key mismatch error. The mismatch caused users to not able to reach the Logon Page.

- **Resolution**
  Engineers issued and installed new matching key pairs. The service was restored at 2:35 AM.

- **Additional Action Items**
  AIS & CTS will pre-validate keys in advance to ensure we are always using the same key at all times.