# Kodowanie i bezpieczeństwo

## Laboratorium - lista nr 9, 2 I

**Zadanie 1 (10 pkt)** Zmodyfikuj działanie serwisu z listy 4. (4 pkt) Zintegruj stronę "bankową" z logowaniem przez: konto Google/profil Facebook/konto Twitter/Windows Live ID (wystarczy integracja z jednym z serwisów).

Jakie korzyści, z punktu widzenia bezpieczeństwa, ma takie rozwiązanie? Jakie zagrożenia dla bezpieczeństwa i prywatności użytkowników rodzi takie rozwiązanie?

(3 pkt) Dodaj do strony zabezpieczenie captcha, o które będzie proszony użytkownik przed rozpoczęciem procesu logowania (wykorzystaj np. reCAPTCHA `http://www.google.com/recaptcha/intro/index.html`).

(3 pkt) Dodaj możliwość "odzyskiwania" hasła, postępuj zgodnie z sugestiami ze strony: `https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet`.

**Zadanie 2 (5 pkt)** Zmodyfikuj sposób generowania kluczy RSA w programie z listy 6. Do wygenerowania mają być wykorzystywane wyłącznie *safe primes* (liczba pierwsza $p$ jest *safe prime* jeżeli jest postaci $p = 2q + 1$ dla pewnej liczby pierwszej $q$).

Przed którymi algorytmami faktoryzacji chroni taka modyfikacja? Porównaj czas generowania kluczy przed i po wprowadzeniu modyfikacji.

**Zadanie 3 (5 pkt)** Zmodyfikuj działanie generowania kluczy RSA w programie z listy 6. Czas działania generowania ma być taki jak czas generowania w zadaniu 2. Teraz jednak postaraj generować się "złe" liczby pierwsze: tj. postaraj się, aby wygenerowany moduł $N = pq$ był podatny na faktoryzację (niech np. $p$ będzie takie, że $p - 1 = \Pi_{i=1}^{k} p_i^{e_i}$, że $max\{p_i\}$ jest stosunkowo mały (np. rzędu $N^{1/4}$).