3 (a)

AcmeHosting.com/[sitename] is the better option from a security perspective. This is because it has a different domain from the online bank AcmeBank.com. If AcmeBank.com/sites/[sitename] is chosen, then this means that it has the same domain name as AcmeBank.com, and a cookie set for AcmeBank.com will be sent automatically by the browser to AcmeBank.com/sites/[sitename] since the cookie's path is a prefix of the URL's path.

3 (b)

(i) The domain of the _ _utma cookie is acme.com. The domain set for the cookie should be a suffix of the webserver's hostname, hence all the website with the domain acme.com that the user visits will be tracked.

(ii) The attacker can craft the script so that the cookies are sent to him instead through a stored XSS attack. After the script has been altered by the attacker, the browser of a user of acme will execute malicious script, telling the Google server to send him all the cookies stored. To prevent the attacker from accessing the other Acme cookies, set the HTTPOnly flag on all the cookies so that scripting languages cannot access or manipulate the cookie.

(iii) Yes, this is because by blocking third-party cookies, since Google Analytics has a different domain from acme.com and hence, outside of the scope of the cookie. Therefore, by the cookie policy, it will now not be able to track the user.

(iv) No it does not prevent Acme from using Google Analytics for tracking their visitors. The Do Not Track header can just be ignored and Google Analytics can still access the cookies. Unless the header can control access of cookies (like the HTTPOnly flag), user's wish to opt out of tracking can be ignored.

3(c)

(i) Eve can steal all of Alice's accounts' information through session hijacking. Firstly, Eve can make Alice to be redirected to http://AcmeBank.com when she visits the https://evil.com/ website. With this, the browser will transmit unencrypted all the cookies for the domain AcmeBank.com as the scope of the cookies will only look at the hostname and path, and not the protocol. After receiving the cookie, Eve can obtain the session token and perform the session hijacking to act as Alice, in which the accounts' information will be displayed.

(ii) To prevent this, set the cookies' Secure attribute to ensure that the cookie is sent to the server only with an encrypted request over the HTTPS protocol, never with unsecured HTTP.